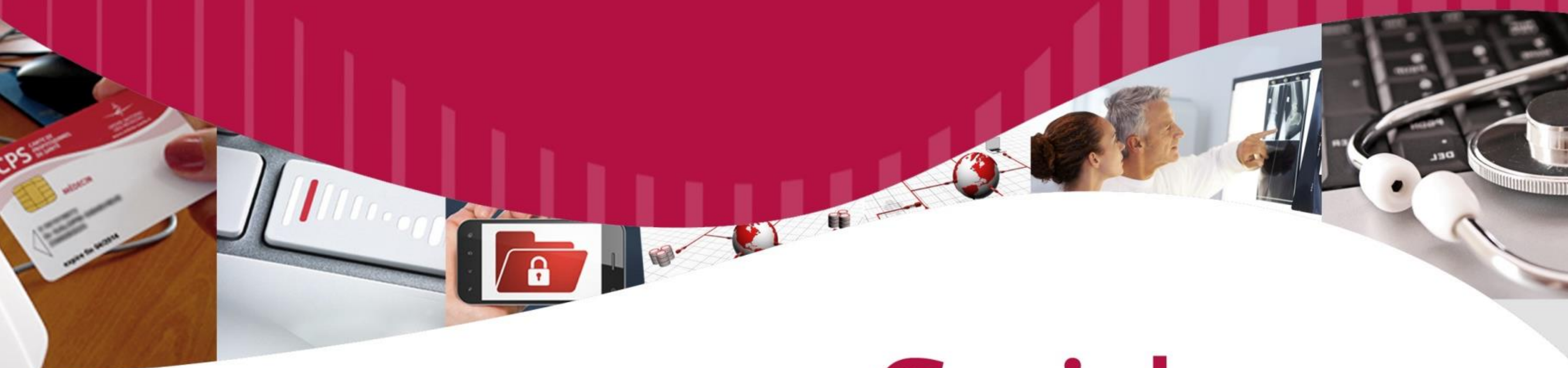


Guide

de **mise en oeuvre** d'un Smartcard logon avec une carte CPS

asipsanté

AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

Version 2.5.8 du 24/09/2014

ASIPSANTÉ
AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

Guide de mise en œuvre d'un Smartcard logon avec une Carte de Professionnel de Santé (CPS)

« ASIP Santé / PTS / PSCE »

Version 2.5.8 du 24/09/2014

Agence des systèmes d'information partagés de santé
9, rue Georges Pitard - 75015 Paris
T.+33 (0)1 58 45 32 50
esante.gouv.fr
Agir ensemble pour soigner mieux

Historique du document			
Version	**Date**	**Auteur**	**Commentaires**
2.5.5	03/12/2013	ASIP	+ Suppression AT_0100 (Citrix) : retrofit dans doc installation/utilisation Cryptolib CPS + Nouvelle 1er de couverture
2.5.6		ASIP	+ Paragraphe « Configuration Smartcard logon sur comptes AD existants » + Paragraphe « Projet » + Paragraphe « Smartcard logon linux » + Paragraphe « Smartcard logon Mac OS X »
2.5.7		ASIP	+ Certificats ASIP Santé PFCNG
2.5.8	24/09/2014	ASIP	+ Références à WSUS et au KRA + Détails installation rôle RDP + Vérifications des statuts de certificats online et offline + Ajout d'illustrations ouverture de session avec « hint » + Précisions dans « Configuration Smartcard logon sur comptes AD existants » : cas 1-to-1 et n-to-m

2 Références

Documents de référence		
ID	**Titre**	**Auteur**
[1]	The Smart Card Cryptographic Service Provider CookBook	Microsoft
[2]	Installation/configuration du provider de révocation de l'ASIP Santé	Microsoft
[3]	Guide_de_deploiement_de_louverture_de_session_par_carte_CPSv3_v1.0.pdf	Microsoft
[4]	ASIP-PTS-PSCE_Manuel-Installation-utilisation-Cryptolib-CPS_20140930_v5.0.9.pdf	ASIP Santé
[5]	ReleaseNote_Public_Cryptolib_Win_v5.0.13.pdf ReleaseNote_Public_Cryptolib_Win_v5.0.13_x64.pdf	ASIP Santé
[6]	Instructions pour l'activation de l'ouverture de session par carte à puce avec des autorités de certification tierces (KB281245)	Microsoft
[7]	Certificate Enumeration	Microsoft
[8]	Microsoft Lifecycle (politique de support Microsoft)	Microsoft

3 Résumé

Ce guide présente la mise en œuvre du **Smartcard logon Windows** avec la carte CPS3 de l'ASIP Santé.

Le **Smartcard logon** permet d'ouvrir une session Windows en utilisant une carte à puce comme vecteur d'**authentification forte** de l'utilisateur.

La **carte à puce** se substitue alors au traditionnel couple login / mot de passe. Ceci permet d'adresser des cas d'usage liés aux milieux/contraintes professionnels (accès en mode « console », accès en mobilité, mise en sécurité du poste sur arrachage carte).

La carte **CPS3** diffusée par l'ASIP Santé est **compatible** avec ce mécanisme à condition qu'elle soit **insérée** dans un lecteur de cartes à puces de type **PC/SC**.

Ce guide documente un « **Kit de Smartcard Logon** » qui est désormais distribué par l'ASIP Santé en complément de ce guide. Ce kit contient les ressources nécessaires aux différentes actions de configuration (certificats et containers de certificats ASIP Santé en particulier).

La mise en œuvre du **Smartcard logon Windows** avec la **carte CPS3** s'appuie sur l'utilisation de la **Cryptolib CPS v5** diffusée par l'ASIP Santé.

Les **Cryptolib CPS v5** sont **indispensables** pour mettre en œuvre le **Smartcard logon Windows** avec la carte **CPS3**. Ce guide et le kit associé ont été conçus en utilisant cette version.

Les **Cryptolib CPS v5** sont des composants logiciels installés sur les postes de travail ainsi que sur les serveurs Microsoft permettant aux systèmes d'exploitation de tirer pleinement profit des fonctionnalités offertes par la carte CPS3 et notamment d'exploiter les fonctionnalités offertes par les volets IAS-ECC (signature, authentification) et sans contact de cette carte.

Cette version de la Cryptolib CPS gère aussi les anciennes cartes CPS2ter qui auront disparu du terrain d'ici mars 2014. Par contre, **seules les cartes CPS3 diffusées depuis mars 2011** permettent de faire du Smartcard logon, les certificats contenus dans les cartes CPS2ter ne présentant pas les caractéristiques requises pour activer cette fonctionnalité.

Les Cryptolib CPS v5 **64bit** sont nécessaires sur les **systèmes 64bit**, qui se démocratisent.

Ce guide et ce kit s'adresse :

- aux développeurs et architectes désireux de s'approprier ou d'évaluer la technologie du Smartcard logon
- aux architectes, chef de projets, DSI ou chef d'établissement ayant besoin d'évaluer les tâches et les charges liées à la mise en place de solutions s'appuyant sur le Smartcard logon
- aux éditeurs de logiciels, quelles que soient leurs tailles, qui souhaitent proposer des solutions intégrant ce type de fonctionnalité ou qui souhaitent pouvoir proposer cette solution en tant que projet d'intégration à leurs clients.

Ce document est une refondation de la version 1.4.0 du guide disponible sur le site intégrateurs de l'ASIP Santé et complète le guide rédigé par Microsoft en collaboration avec l'ASIP Santé (cf. **[3]**, avec des indications en anglais).

Le document s'organise en 5 parties :

1. Présentation générale du Smartcard Logon
2. Prérequis et Configurations requises (aspects généraux)
3. Mise en œuvre détaillée, en pas à pas, en français, sur une architecture simple (Annexe 6)
4. Limitations connues et contournements
5. Descriptif du « Kit Smartcard logon ASIP Santé »

4 Sommaire

2 Références 4

3 Résumé 5

4 Sommaire 6

5 Glossaire 9

6 Liste des entreprises citées 10

7 Avertissements 11

8 Introduction 12
- 8.1 Objectifs 12
- 8.2 Présentation générale du Smartcard logon 12
- 8.3 Intérêt du Smartcard logon 14

9 Architecture et fonctionnement général 16
- 9.1 Schéma de principe 16
- 9.2 Fonctionnement général 19
  - 9.2.1 Protocole Kerberos 19
  - 9.2.2 Protocole PKINIT 21
  - 9.2.3 Cinématique initiale 21
- 9.3 Smartcard logon et services de terminal 22

10 Spécifications matérielles et prérequis 23
- 10.1 Architecture « serveur » 23
  - 10.1.1 Composants 23
  - 10.1.2 PKI et Autorités de certification 25
- 10.2 Architecture « client » 27
  - 10.2.1 Matériel 27
  - 10.2.2 Logiciel 27
  - 10.2.3 Cartes et certificats 27

11 Configuration 30
- 11.1 Configuration du poste client 30
- 11.2 Configuration Serveur allégée 33
- 11.3 Configuration d'un contrôleur de domaine 33
- 11.4 Configuration du serveur de certificats (PKI Microsoft) 36
- 11.5 Configuration des options de sécurité 37
  - 11.5.1 Forcer l'utilisation de la carte à puce 37
  - 11.5.2 Comportement du système au retrait de la carte à puce 38
  - 11.5.3 Forcer l'approbation du contrôleur de domaine à l'ouverture de session 38
  - 11.5.4 Désactivation de la vérification des CRLs 39
- 11.6 Exemple pratique d'une configuration de serveur 40
- 11.7 Exemples d'architecture réseau 43

12 Annexes 44
- 12.1 Maquette de Smartcard logon avec une carte CPx 44
  - 12.1.1 « Brief Project » 44
  - 12.1.2 Ressources nécessaires 45
  - 12.1.3 Livrables 46
  - 12.1.4 Macro-Planning 46
  - 12.1.5 Remarques 48
- 12.2 Installation du poste de travail client 49

12.3 Installation de Windows 2008 R2 SP1 ... 58
12.4 Installation d'un rôle Active Directory ... 69
12.5 Installation d'un rôle Certificate Server ... 85
12.6 Installation d'un rôle Terminal Server ... 99
12.6.1 Installation des composants du rôle Terminal Server ... 99
12.6.2 Activation du serveur de licence RDP ... 106
12.6.3 Configurations des comptes « Serveurs de licences des services Terminal Serveur » 108
12.6.4 Installation des licences sur le serveur de licences ... 108
12.6.5 Configuration de l'hôte Terminal Server ... 111
12.6.6 Paramétrage du serveur RDP ... 113
12.6.7 Configuration du certificat du serveur RDP ... 120
12.6.8 Autres GPOs ... 132
12.7 Installation d'un rôle IIS ... 134
12.8 Installation de la Cryptolib CPS sur le serveur ... 138
12.8.1 Désactivation du CCM au lancement ... 138
12.8.2 Activation du CCM à l'ouverture de session au cas par cas ... 138
12.8.3 Remarque sur le provisionning des magasins de certificats ... 138
12.9 Installation du Provider de révocation ASIP Santé – Microsoft sur le serveur ... 139
12.9.1 Installation du Provider de révocation ASIP Santé – Microsoft ... 139
12.9.2 Mise à jour des magasins de certificats Local Machine ... 141
12.9.3 Configuration du Provider de révocation ASIP Santé – Microsoft ... 145
12.9.4 Cas des contrôleurs de domaine avec accès internet : vérification des statuts de certificats « online » ... 146
12.9.5 Cas des contrôleurs de domaine sans accès internet : vérification des statuts de certificats « offline » via l'alimentation du magasin de CRL en ligne de commande ... 146
12.9.6 Test du Provider de révocation ASIP Santé – Microsoft en vérifiant le statut d'un certificat 148
12.10 Configuration d'une console de composants enfichables dédiée au Smartcard logon ... 151
12.11 Configuration du Contrôleur de domaine pour la Smartcard logon ... 160
12.11.1 Magasins de certificats ... 160
12.11.2 Stratégie Active Directory ... 166
12.12 Création des utilisateurs ... 168
12.12.1 Construction de l'identifiant UPN ... 168
12.12.3 Déclaration du suffixe carte-cps.fr dans l'AD ... 170
12.12.4 Déclaration d'un utilisateur ... 171
12.13 Paramétrage du Smartcard logon sur des nouveaux comptes AD ... 174
12.13.1 Script de déploiement des UPNs dans un active directory ... 174
12.14 Paramétrage du Smartcard logon sur des comptes AD préexistants ... 177
12.14.1 Cas "1-to-1" : {un compte existant ; une carte} ... 177
12.14.2 Cas "n-to-m" : mappages de comptes existants sur des attributs de certificats X509 [Win2008R2] ... 178
12.14.3 Cas "n-to-m" : Désactivation de l'utilisation du subjectAltName (SAN) ... 182
12.14.4 Cas "n-to-m" : Activation du « hint » ... 182
12.14.5 Cas "n-to-m" : Interface de logon et ergonomie ... 184
12.15 Configuration de la stratégie de détection d'arrachage de la carte ... 185
12.16 Détails des certificats ASIP Santé ... 188
12.17 Debugging ... 201
12.17.1 Traces Cryptolib CPS ... 201
12.17.2 Traces Kerberos ... 201
12.18 Points d'attention et contournements ... 204
12.18.1 Limitations ... 204
12.18.2 Contournements ... 211

13 Contenu du « Kit Smartcard logon ASIP Santé » 214
14 Smartcard logon sous Linux 217
14.1 Installation de la Cryptolib CPS v5 pour Linux 217
14.2 Configuration du lancement automatique du daemon PCSCD 217
14.3 Installation et configuration du PAM OpenSC 217
14.3.1 Récupération et installation de libpam-pkcs11 217
14.3.2 Initialisation du fichier pam_pkcs11.conf, des certificats et des CRLs 218
14.3.3 Edition de /etc/pam.d/sudo 218
14.3.4 Edition de /etc/pam.d/common-auth 218
14.3.5 Edition de /etc/pam_pkcs11/pam_pkcs11.conf 219
14.3.6 Configuration d'un compte pour le Smartcard logon 219
15 Smartcard logon sous Mac OS X 220
15.1 Pré-requis 220
15.2 Méthode 220
15.3 Autres commandes utiles 220
15.4 Remarques 221
16 Annexe – Liste des figures 222
17 Annexe – Liste des tables 226
18 Notes 228

5 Glossaire

Sigle	Signification
API	Application Programming Interface
ATR	Answer to reset : Réponse d’une carte à puce à sa mise sous tension.
CPS	Carte de Professionnel de Santé
CSP	Cryptographic Service Provider : Bibliothèque logicielle de fonctions cryptographiques fournie par Microsoft ou un éditeur tiers (fournisseur de carte).
Kerberos	Protocole d’authentification réseau, basé sur l’utilisation de tickets. Utilisé par défaut à partir de Windows 2000.
KRA	Microsoft Key Recovery Agent
MSGINA / GINA	Microsoft GINA (Graphical Identification And Authentification): DLL standard Microsoft gérant l’interface graphique utilisateur, lors de l’ouverture de session. Elle se charge notamment de demander à l’utilisateur le code porteur de sa carte.
MSI	Microsoft Installer : Format de fichier d’installation de Microsoft, géré par le moteur d’installation Windows Installer.
NTAuth	Magasin de certificats d’un poste Windows client, alimenté exclusivement par le contrôleur de domaine par propagation. Contient les certificats d’autorités de confiance. Utilisé par Winlogon.
PC/SC	Personal Computer/Smart Card : Bibliothèque logicielle standard pour l’accès aux lecteurs et aux cartes à puce.
PDC	Primary Domain Controller : Contrôleur de domaine principal.
PKI (IGC)	Public Key Infrastructure (Infrastructure de Gestion des Clefs)
SI	Système d’information : Ensemble organisé de ressources (matériels, logiciels, personnel, données et procédures)
TSE	Terminal Server Edition : Service de Terminal de Microsoft. Composant permettant d’accéder à des applications et des données sur un ordinateur distant au travers de n’importe quel type de réseau.
RDP	Remote Desktop Protocol : Protocole de communication utilisé par TSE.
WSUS	Windows Server Update Services

Tableau 1 : Glossaire

6 Liste des entreprises citées

Le présent document cite les produits des entreprises ou organismes suivants:

Nom	Site Web	Lien avec le Smartcard logon
Apple	www.apple.com	**Mac OS X**
Citrix	www.citrix.com	**Env. TSE/Citrix**
Debian	www.debian.org	**Linux, .deb**
Microsoft	www.microsoft.com	**Windows, CSP, TSE, AD DC, AD CS**
PC/SC Workgroup	www.pcscworkgroup.com	**Responsable du standard PC/SC visant l'intégration de la carte à puce et des lecteurs de cartes dans les systèmes informatiques**
Redhat	www.redhat.com	**Linux, .rpm**
RSA Security Inc.	**www.rsa.com**	**PKCS, RSA**

Tableau 2 : Entreprises citées

7 Avertissements

Sur le nécessaire strict respect des procédures décrites dans le manuel L'attention de l'utilisateur est attirée sur l'importance de respecter strictement les procédures décrites dans le présent guide de mise en œuvre du Smartcard logon avec une carte CPS. Toutes les procédures qui y sont décrites ont été préalablement testées par l'ASIP Santé. Elles doivent permettre à l'utilisateur de mettre en œuvre le Smartcard logon avec une carte CPS sur son poste de travail ou tout autre dispositif informatique. En cas de non-respect de ces procédures et des conditions normales d'utilisation des composants logiciels mentionnés dans ce guide, sa mise en œuvre est susceptible d'engendrer des dysfonctionnements dans l'environnement de travail de l'utilisateur. En cas de dysfonctionnement, quel qu'il soit, l'ASIP Santé prêtera dans la mesure du possible assistance à l'utilisateur, qui ne pourra rechercher sa responsabilité en cas de non-respect des procédures décrites dans le présent manuel.
Sur les liens externes Le présent guide contient des liens vers des sites Internet. Ces liens ne visent qu'à informer l'utilisateur. Ces sites Web ne sont pas gérés par l'ASIP Santé et l'ASIP Santé n'exerce sur eux aucun contrôle : leur mention ne saurait engager l'ASIP Santé quant à leur contenu. L'utilisation des sites tiers mentionnés relève de la seule responsabilité du lecteur ou de l'utilisateur des produits documentés.
Sur les copies d'écran et les lignes de commande Les lignes de commandes données ci-après le sont à titre indicatif. Elles documentent des cas « passants » qui peuvent différer d'un système à l'autre. Les copies d'écran présentées dans ce document sont données à titre illustratif. Les pages ou écrans réellement affichés peuvent être différents, notamment en raison de montées de version ou de configurations d'environnements différentes.
Citations L'ASIP Santé est contrainte de citer le nom de certaines entreprises recensées au tableau n°2 afin d'apporter toute l'aide nécessaire aux utilisateurs désireux de mettre en œuvre le Smartcard logon avec une carte CPS. Les entreprises citées peuvent prendre contact avec l'ASIP Santé à l'adresse email editeurs@asipsante.fr pour toute demande en lien avec la citation les concernant. Les entreprises non citées dans ce manuel et ayant une activité en lien avec le Smartcard logon CPS peuvent également se faire connaître auprès de l'ASIP Santé en la contactant à la même adresse.
Contact Toute question en rapport avec le contenu du présent guide doit être adressée à l'adresse suivante: editeurs@asipsante.fr

Tableau 3 : Avertissements

8 Introduction

8.1 Objectifs

L'objectif de ce document est d'accompagner le déploiement d'un mécanisme d'ouverture de session Microsoft Windows à partir d'une carte à puce de la famille CPS.

Ce document décrit les bonnes pratiques pour un déploiement d'un mécanisme de Smartcard logon sur un réseau Microsoft.

Il n'est pas exhaustif : toutes les architectures clientes existantes ou futures ne sont pas couvertes. Il adresse cependant les principales architectures « standards ».

Il vise la réussite de la mise en place d'une architecture simple de Smartcard logon.

Il est basé sur les expériences de l'ASIP Santé dans ce domaine. Il regroupe les différentes techniques de configuration standard au Smartcard logon, adaptées à l'utilisation de la carte CPS.

Il contient des tableaux récapitulatifs qu'il est utile d'imprimer afin d'appliquer au mieux le paramétrage requis.

8.2 Présentation générale du Smartcard logon

Il est possible depuis Microsoft Windows 2000 de remplacer la saisie du couple login / mot de passe par une authentification par carte à puce au moment de réaliser une ouverture de session Windows dite « interactive ».

Tout réseau utilisant Active Directory et un contrôleur de domaine Microsoft (Windows Server 2000, 2003 ou 2008) peut bénéficier de la technologie "Smartcard logon" en standard.

Ce mécanisme d'ouverture de sessions Windows par carte à puce est par ailleurs compatible avec les sessions Terminal Services TSE (voir chapitre « **Smartcard logon et les services de terminal** »).

Le principe de base de ce mécanisme est une authentification mutuelle entre la carte présente dans un lecteur du poste client et le serveur du domaine à partir de certificats électroniques X.509. Le lecteur de carte doit impérativement être de type PC/SC.

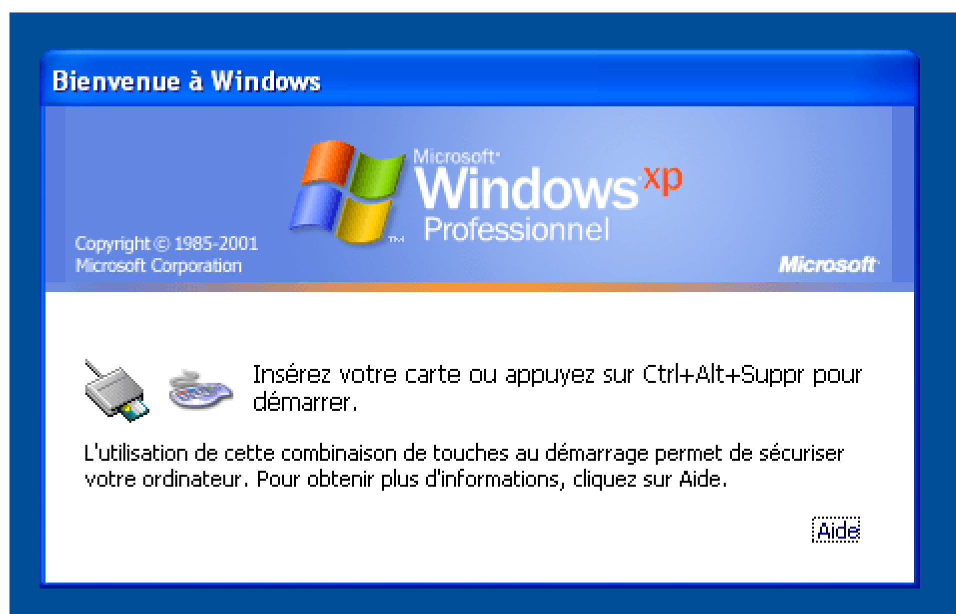


Figure 1 : Ecran d'accueil de Windows XP, configuré pour ouvrir une session avec une carte à puce.

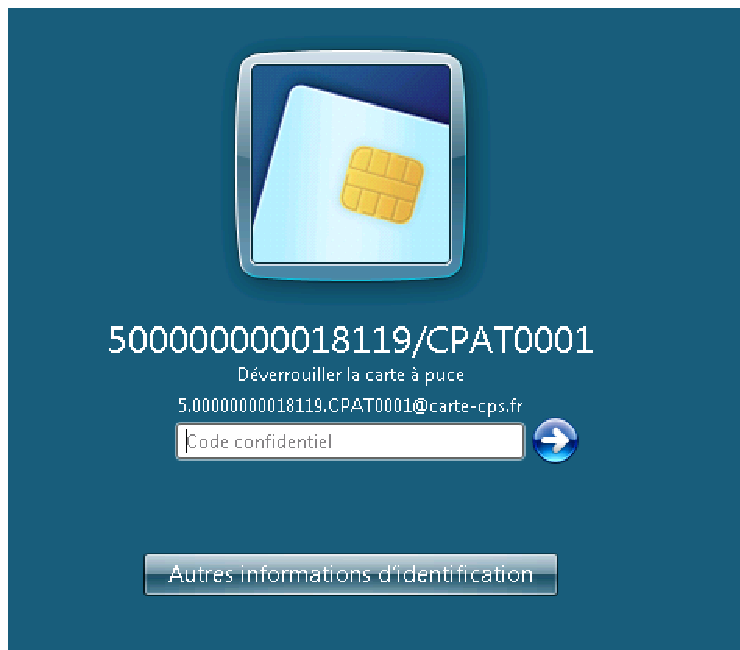


Figure 2 : Ecran d'accueil de Windows 7, configuré pour ouvrir une session avec une carte à puce.

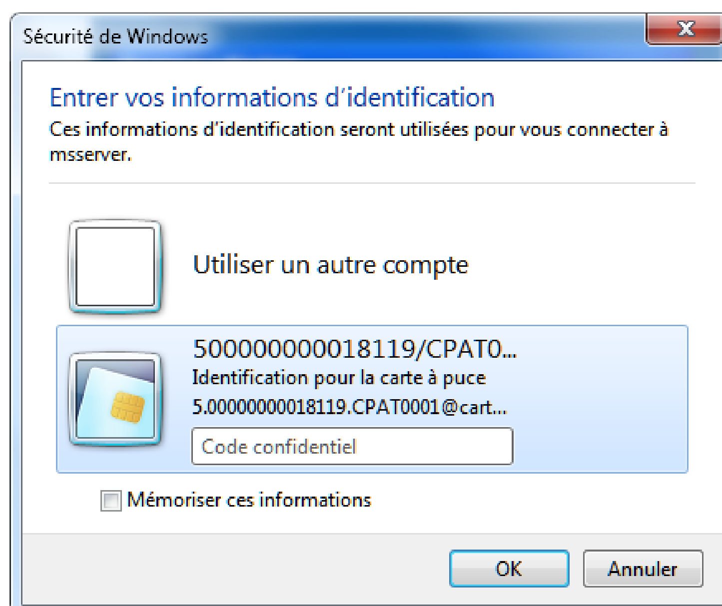


Figure 3 : Ecran du client Terminal Server sous Windows 7 pour ouvrir une session avec une carte à puce.

8.3 Intérêt du Smartcard logon

Cette section analyse les raisons d'utiliser une carte à puce (de type CPS par exemple) plutôt qu'une authentification standard login/mot de passe pour l'ouverture de session utilisateur.

Inconvénients login-mdp	Description
I_0010	Mot de passe faible (choisi par l'utilisateur), facilement « crackable » (attaque par dictionnaire par exemple)
I_0020	Algorithmes LM/NTLM/NTLMv2 faibles
I_0030	Systèmes de sécurité logiciels cassables (récupération des mots de passe dans la SAM, « KeyLoggers », …)
I_0040	Multiplication des mots de passe

Tableau 4 : Inconvénients du couple login/mot de passe

Avantages carte à puce	Description
I_0050	La clé est générée par le système (pas de clé faible)
I_0060	Les algorithmes sont robustes
I_0070	La longueur de clé est importante
I_0080	La clé privée est stockée dans la carte et ne peut pas être extraite
I_0090	Le certificat de l'utilisateur devient son identité numérique
I_0100	Cette identité est standard : elle suit des normes et des préconisations normalisées, reconnues et largement adoptées par ailleurs.
I_0110	La phase de login fait intervenir 2 facteurs d'authentification différents : 1. « ce que j'ai » : la carte CPS 2. « ce que je saisi » : le code porteur de la carte CPS L'authentification est dite « **forte** ».

Tableau 5 : Avantages de la carte à puce

Inconvénients carte à puce / login-mdp	Description
I_0120	Architecture parfois délicate à mettre en place (PKI serveur, accès externe à un annuaire, installation matérielle et logicielle du poste…)
I_0130	Ouverture de session un peu plus longue (de l'ordre de quelques secondes supplémentaires, en fonction de la vitesse d'accès et de calcul de la carte, et du poste client). Ces temps sont optimisés avec la Cryptolib CPS v5 via l'utilisation d'un cache de certificats.
I_0140	Administration plus complexe de l'architecture (gestion des PKI, gestion des flux externes, expiration des certificats, …)

Tableau 6 : Inconvénients de la carte à puce face au couple login/mot de passe

Les inconvénients d'ordre technique liés à la mise en œuvre de la carte à puce sont mineurs par rapport aux avantages (notamment en terme de sécurité) apportés par cette technologie et au regard des limitations et faiblesses avérées du login/mot de passe.

9 Architecture et fonctionnement général

9.1 Schéma de principe

Le mécanisme d'ouverture de session Windows est illustré ci-dessous.

Ce mécanisme est complexe par essence. Les considérations de sécurité y prévalent, conjointement aux considérations de performance qu'il faut introduire sans compromettre le système.

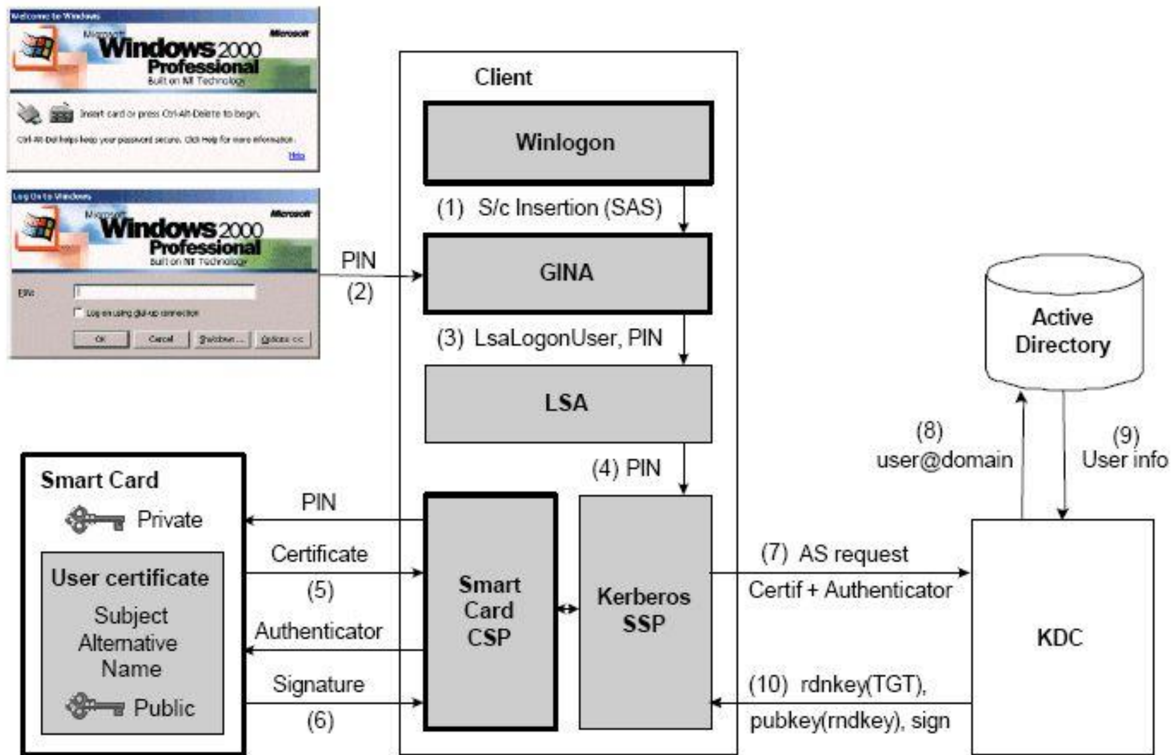


Figure 4 : Schéma fonctionnel global du Smartcard logon de Microsoft (Win 2000 et XP)

Microsoft a revu ce mécanisme lors de la sortie de Windows Vista.
Si la logique du mécanisme reste sensiblement la même, l'implémentation change avec la disparition de MS Gina et l'apparition du composante Base CSP / Minidriver.

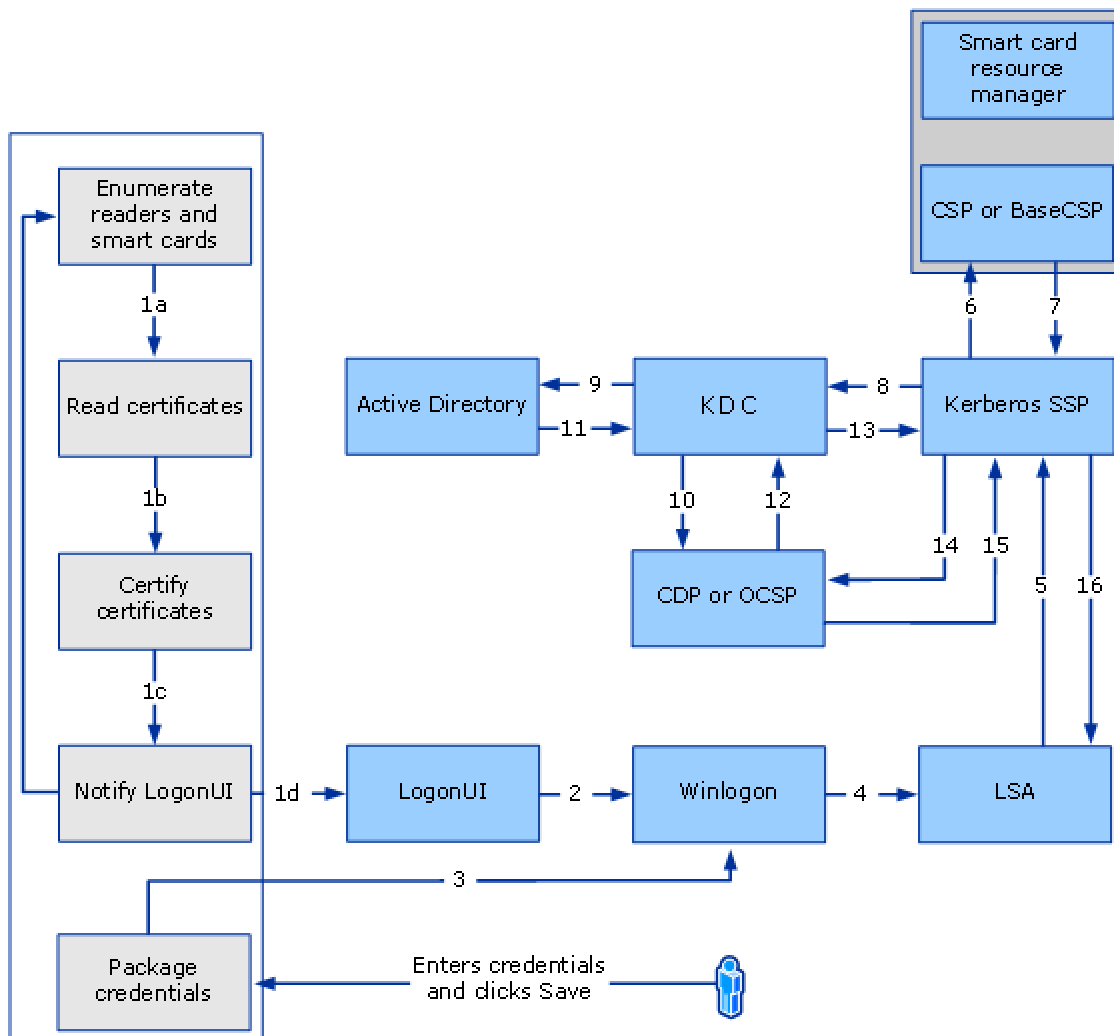


Figure 5 : Schéma fonctionnel global du Smartcard logon de Microsoft (Win Vista+) [7]

Composant	Description
MSGINA	[Windows XP] Microsoft GINA (Graphical Identification And Authentification) = Bibliothèque standard Microsoft gérant l'interface graphique utilisateur, lors de l'ouverture de session. Elle se charge notamment de demander à l'utilisateur le code porteur de sa carte.
LSA	Local Security Authority : il s'assure que l'utilisateur à la permission d'accéder au système. Il crée les jetons d'accès. C'est lui qui lance le processus d'authentification du module Kerberos.
Kerberos SSP	(Kerberos Security Support Provider) : DLL principale intervenant dans le processus d'ouverture de session entre un client et un serveur (le protocole standard actuel est appelé Kerberos V5, normalisé par l'IETF dans les RFC 1510). Elle intervient aussi bien dans une ouverture de session standard (avec logon/mot de passe), que dans une ouverture par carte à puce (PKINIT).
KDC	Key Distribution Center = Centre de distribution des clés. Module serveur implémenté par le protocole Kerberos (pour l'authentification et l'autorisation des utilisateurs distants).
PAC	Privilege attribute certificate : contient les informations à destination du client telles que : le SID (User security ID), les droits de l'utilisateur sur le domaine.

Tableau 7 : Smartcard logon: Principaux Composants Microsoft mis en œuvre

Mettre en œuvre le Smartcard logon revient à configurer chaque acteur impliqué dans ce mécanisme.

9.2 Fonctionnement général

9.2.1 Protocole Kerberos

L'ouverture de session Windows repose sur le protocole d'authentification réseau Kerberos qui gère aussi bien, via le protocole PKINIT, l'authentification par login/password que par carte à puce.

Voici, schématiquement le fonctionnement du protocole **Kerberos V5** lors de l'ouverture de session:

Un système Kerberos fait intervenir les **trois sous protocoles suivants**:

1. **AS** (Authentication Service)
2. **TGS** (Ticket-Granting Service)
3. **CS** (Client/Server)

Les échanges de données entre le client et le serveur se font par des messages de requêtes/réponses normalisés suivant le protocole Kerberos suivant :

Etape	Code	Communication	Description
1	KRB_AS_REQ	Client > Serveur	Requête de service d'authentification Kerberos. (Vérification de l'identité du client) Le certificat d'authentification (présent dans la carte) est sursigné par sa propre clé privée et envoyé, accompagné de données relatives au client, du poste client vers le serveur.
2	KRB_AS_REP	Serveur > Client	Réponse du serveur. Le serveur envoie au client, en cas d'authentification réussie, une clé de session (clé symétrique) et un TGT (Ticket d'accès au service de délivrement de ticket, limité dans le temps). Le tout chiffré avec la clé publique du client (envoyée dans le message de requête).
3	KRB_TGS_REQ	Client > Serveur	Requête de ticket de session au serveur de ticket (Chiffrée par la clé de session). Envoi du TGT dans la requête.
4	KRB_TGS_REP	Serveur > Client	Réponse du serveur. Envoi du ticket de session au client (Ticket d'accès au serveur)
5	KRB_AP_REQ	Client > Serveur	Requête applicative. Envoi du ticket de session.
6	KRB_AP_REP	Serveur > Client	Réponse du serveur. La session peut être ouverte. Les échanges peuvent se poursuivre entre le client et le serveur.

Tableau 8 : Smartcard logon: Protocole Kerberos

9.2.2 Protocole PKINIT

Le scénario d'ouverture d'une session Windows à partir d'une carte à puce (Smartcard logon) suit une procédure stricte définie par Microsoft.

La procédure complète est décrite dans le document : **The Smart Card Cryptographic Service Provider CookBook [1]** disponible en accès libre sur le site de Microsoft.

Ce protocole est appelé PKINIT. PKINIT est une extension du protocole Kerberos qui rend possible l'utilisation de certificats numériques X509 pour la phase d'authentification. Cette extension permet en particulier de remplacer l'authentification login/mot de passe par une authentification par carte à puce.
Il définit précisément les échanges entre la carte (via le CSP et PC/SC) et Kerberos (via Winlogon).

9.2.3 Cinématique initiale

La cinématique réalisée lorsqu'une carte à puce est insérée dans un lecteur d'un poste configuré pour le Smartcard logon est la suivante :

Etape	Description
C_0010	Une carte est insérée dans un lecteur PC/SC du poste client.
C_0020	Le service **ScardSvr** du poste client (service Windows « **Smartcard Server** » : gestionnaire des lecteurs de carte sur le poste) détecte cette insertion via **Winscard.dll** (bibliothèque de gestion PC/SC de Microsoft « **Smartcard API** »).
C_0030	Le processus Winlogon est réveillé par le service **ScardSvr**.
C_0040	Winlogon envoie une commande de demande d'ATR à la carte (via le gestionnaire de cartes).
C_0050	Winlogon reçoit l'ATR et recherche en base de registres, s'il existe une association avec un CSP dans la table de correspondance ATR<->CSP.
C_0060	Si un CSP est trouvé, Winlogon va demander (via GINA sous Windows XP), le code porteur à l'utilisateur.
C_0070	Il va ensuite demander à récupérer le certificat d'authentification de la carte (en passant à la carte le code porteur rentré par l'utilisateur, via le CSP associé).
C_0080	Winlogon peut alors lancer le processus **Kerberos** (via **LSA**) qui va exécuter la procédure d'authentification/vérification du client par le serveur de domaine, par carte à puce (protocole **PKINIT**), et lui renvoyer le certificat d'authentification récupéré dans la carte.
C_0090	Si toute la procédure s'est déroulée correctement (identification/authentification correcte de l'utilisateur par le contrôleur de domaine), l'utilisateur est alors autorisé à ouvrir une session sur le poste client.

Tableau 9 : Smartcard logon: Cinématique de l'authentification par carte à puce

9.3 Smartcard logon et services de terminal

Le mécanisme d'ouverture Windows par carte à puce (Smartcard logon) est compatible avec les sessions Terminal Services TSE, bureau à distance (qui s'appuient sur le protocole RDP) et architecture CITRIX (protocole ICA).

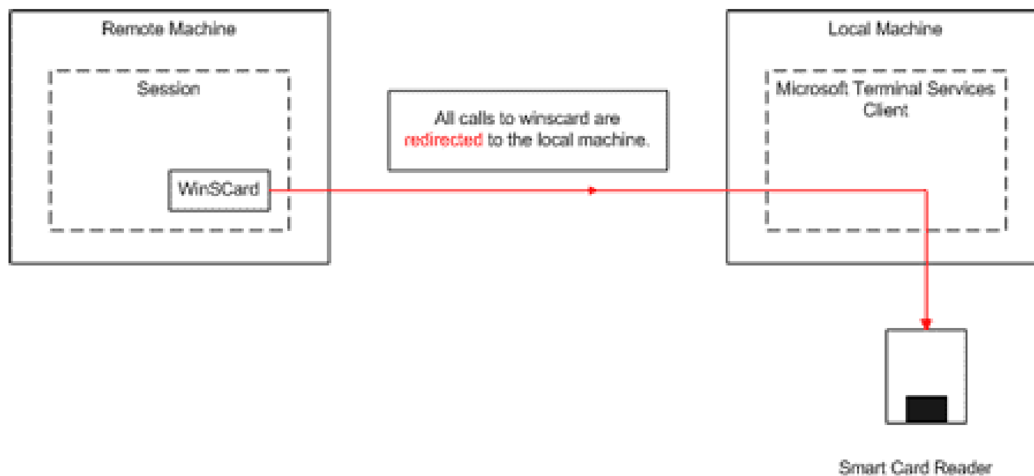


Figure 6 : Smartcard logon et TSE : Redirection des APDU [1]

Il est donc possible d'ouvrir nativement une session client/serveur à distance par carte à puce (à partir d'un client dit « léger »).

La connexion à distance doit être configurée pour qu'elle utilise le(s) lecteur(s) de cartes à puce PC/SC présents sur le poste client (redirection carte à puce, PC/SC).

10Spécifications matérielles et prérequis

10.1 Architecture « serveur »

10.1.1 Composants

Composant	Description
COMP_01	Un réseau informatique « Microsoft » : postes clients Windows (à partir de Windows 2000), intégrés à un domaine géré par un ou des contrôleur(s) de domaine Windows.
COMP_02	Au moins un serveur avec le rôle de contrôleur de domaine (Windows 2000 Server, 2003 Server ou supérieur) avec un Active Directory (gestion des utilisateurs).
COMP_03	Des contrôleurs de domaine secondaires peuvent être présents sur le domaine. Dans ce cas, la configuration spécifique au Smartcard logon devra être reproduite sur chaque contrôleur (pour que chaque contrôleur soit configuré de la même manière).
COMP_04	Composants d'une IGC (PKI) pour les certificats serveur et client : • Un accès externe à l'annuaire de l'ASIP Santé (en http et/ou LDAP), pour permettre au module de vérification de révocation (« Provider de révocation ») d'accéder aux CRLs correspondantes aux certificats délivrés par l'ASIP Santé. • Microsoft Certificate Server (pour une PKI serveur Microsoft) • Provider de révocation ASIP Santé[1] développé par Microsoft pour la vérification des CRLs des certificats client de la carte sur chaque contrôleur de domaine.

Tableau 10 : Smartcard logon: Cinématique de l'authentification par carte à puce

[1] Dans l'IGC de l'ASIP Santé, l'autorité qui signe les certificats est différente de celle qui signe les CRL.

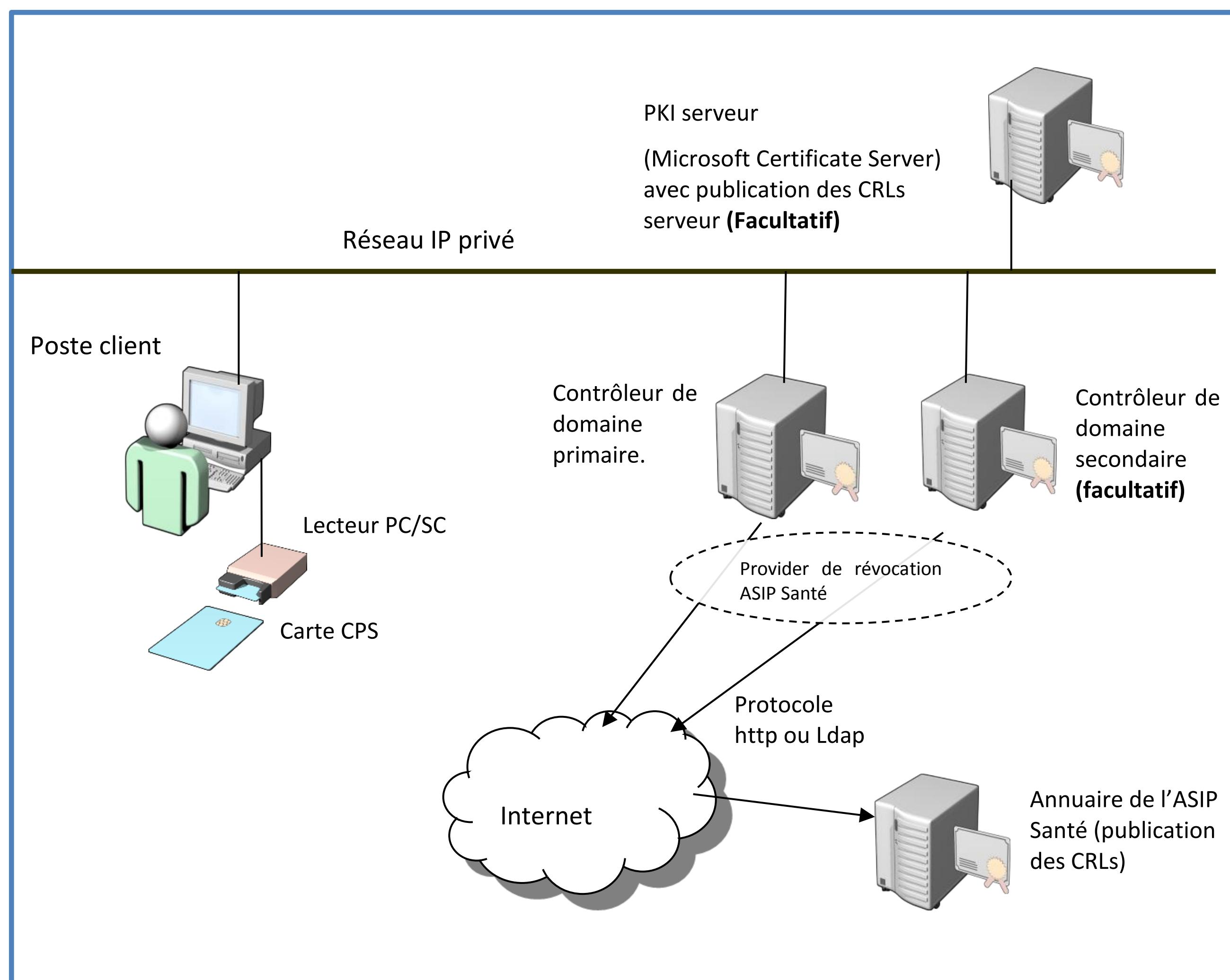


Figure 7 : Architecture: Exemple d'un réseau informatique configuré pour le Smartcard logon

10.1.2 PKI et Autorités de certification

Pour fonctionner, le mécanisme du Smartcard logon effectue une authentification mutuelle entre un poste client et le contrôleur de domaine, basé sur des certificats X509 : le client présente un certificat d'authentification contenu dans la carte, le serveur présente un certificat serveur authentifiant le contrôleur de domaine.

Pour vérifier l'authenticité du certificat client, le serveur vérifie notamment que la chaîne d'autorité de ce certificat est de confiance (Validité structurelle et temporelle du certificat, non révocation, autorités associées valides et non révoquées).

De même pour le client qui vérifie que la chaîne d'autorité du certificat serveur est de confiance.

Pour cela, il faut que chaque entité (client et serveur) possède un certificat associé à une PKI accessible à partir du/des contrôleur(s) de domaine et des postes client.

Lors de la procédure d'ouverture de session par carte à puce, et plus précisément lors de la vérification de la validité des certificats client et serveur (ainsi que leurs autorités), la vérification de la révocation doit être obligatoirement effectuée.

10.1.2.1 PKI cliente

Pour les cartes CPS, la PKI est gérée par l'ASIP Santé.

Les autorités de certification ainsi que les CDPs (point de distribution des CRLs) sont disponibles sur l'annuaire public de l'ASIP Santé.

Ces CRLs seront obligatoirement vérifiées par le composant « **provider de révocation ASIP Santé** » (**CPSRev**) installé sur chaque contrôleur de domaine. Ces vérifications ont lieu à chaque demande d'ouverture de session par un client. En cas d'échec du contrôle, l'utilisateur ne pourra pas ouvrir de session.

Il est possible - mais déconseillé - de désactiver la vérification des CRLs (voir section « **désactivation de la vérification des CRLs** » et annexe 6).

10.1.2.2 PKI serveur

En ce qui concerne la PKI du certificat serveur, plusieurs implémentations techniques sont possibles:

Scénario	Description
1	**PKI Microsoft** composant intégré à Windows 2000 Server, 2003 Server, 2008 Server, 2012 Server : Microsoft Certificate Server ou Active Directory Certificate Server (AD CS) (voir documentation spécifique pour l'installation et la configuration)
2	**PKI ASIP Santé** un certificat serveur généré (type DomainController) + sa chaîne de certification complète certifié par l'ASIP Santé (autorité Classe 4 par exemple (classe des certificats serveur)). Cette PKI est déjà utilisée pour les certificats client.
3	**PKI externe** un certificat serveur généré (type DomainController) + sa chaîne de certification complète de confiance (autre que ASIP Santé).

Tableau 11 : Architecture: Scénarios d'implémentation de PKI serveur

Problématique:

- La chaîne de certification doit avoir des CDP (points de distribution de CRL) à tous les niveaux (certificat final + certificat AC intermédiaire).
  Ce n'est pas le cas de la chaîne du GIP-CPS classe 4.
  La vérification des CRLs étant obligatoire, l'utilisation d'une PKI externe basée sur les autorités de l'ASIP Santé (**cas 2**) semble impossible.
- Le **cas 3** reste possible mais est très fastidieux à mettre en place et à intégrer à l'infrastructure Microsoft.
  Cette option est donc déconseillée, sauf si une PKI existe déjà et est utilisée pour une autre fonction.
- **La solution conseillée est donc le cas 1**, c'est-à-dire d'utiliser **la PKI de Microsoft (Microsoft Certificate Server ou AD CS)**, pour générer et administrer une PKI en local sur le réseau interne. Ce module s'intègre facilement et rapidement à l'infrastructure existante (serveurs Windows, Active Directory), et permet de configurer une PKI, et de générer un certificat serveur (contrôleur de domaine) en très peu de temps.

L'installation de Microsoft Certificate Server met en place et configure automatiquement toute une PKI par défaut, et donc notamment :

- La mise en place des CDPs par publication sur le réseau (accès par LDAP)
- la diffusion des autorités de certification sur toutes les machines du domaine.
- L'autorité d'enregistrement : génération très simple d'un certificat pour un contrôleur de domaine (un certificat serveur de type « Domain Controller » (DC))

10.1.2.3 Format d'un certificat « Domain Controller » (DC)

Ce certificat d'authentification installé sur un serveur de domaine permet l'authentification de ce serveur de domaine par un poste client.

Le certificat DC doit contenir les champs suivants:

- **CDP (CRL Distribution Point).**
- **« Key usage » = Digital Signature, Key Encipherment**
- **« Application policies » =**
  -> Client Authentication (1.3.6.1.5.5.7.3.2)
  -> Server Authentication (1.3.6.1.5.5.7.3.1)
- **« Subject Alternative Name » =**
  -> GUID de l'objet contrôleur de domaine et nom DNS (= identifiant unique du serveur)
- **CSP RSA Schannel pour générer la clé**
- **Gabarit de certificat = DomainController**

Le sujet de l'objet doit être : CN =<dcname> (=le nom du contrôleur de domaine), pour pouvoir être publié dans l'Active Directory du contrôleur de domaine (pour retrouver le chemin de l'AD correspondant).

10.2 Architecture « client »

Une ouverture de session dite « interactive » (ouverture par carte à puce), n'est gérée en natif qu'à partir de Windows 2000. Les systèmes d'exploitation Windows XP, Vista, Seven et Windows 8 supportent ce mécanisme.

Peu de modifications sont donc nécessaires pour faire fonctionner le Smartcard logon.

Le présent paragraphe détaille les conditions requises pour utiliser une carte à puce CPS en ouverture d'une session Windows.

10.2.1 Matériel

- Au moins un lecteur de type PC/SC doit être installé (pilotes spécifiques installés) et présent sur le poste client, (le protocole PC/SC étant une architecture intégrée nativement dans l'OS et qui permet de prendre en compte l'insertion de la carte comme déclencheur de l'ouverture de session)
- Le poste client doit être connecté physiquement à un réseau privé et être déclaré sur un domaine de ce réseau.

L'authentification par carte à puce est une authentification forte établie obligatoirement entre un client et un serveur: une authentification locale sur le poste n'est pas possible.

Remarque: si ces deux prérequis ne sont pas respectés, l'écran d'accueil du poste client (GINA sous Windows XP) ne proposera pas l'insertion carte.

10.2.2 Logiciel

- La GINA (Graphical Identification and Authentication) d'origine.

Pour pouvoir ainsi gérer l'événement insertion carte. Toute autre GINA développée spécifiquement, désactivera la détection carte : par exemple une GINA de gestion biométrique d'empreinte digitale.

Ce pré requis est valable uniquement pour Windows 200 et XP.

A partir de Windows Vista, la GINA n'est plus modifiable, seuls des « credential provider » peuvent être ajoutés.

- Un CSP (Cryptographic Service Provider) d'interface standard et prévu pour dialoguer avec les cartes CPS doit être installé et correctement configuré, ainsi que les APIs correspondantes pour accéder à la carte via le lecteur. **Ce CSP est fourni par l'ASIP Santé dans le setup MSI de la Cryptolib CPS à partir de la version 5 (ou en version PC/SC).**

10.2.3 Cartes et certificats

Pour une utilisation en Smartcard logon, les certificats X509 d'authentification des cartes CPS doivent être de type « Smartcard logon » (SC), c'est-à-dire doivent posséder les champs suivants :

- « Extended Key Usage »
  (OIDs) = Smart Card Logon (**1.3.6.1.4.1.311.20.2.2**)
- « Subject Alternative Name » = UPN = **ID_user@carte-cps.fr**
  (**ID_user** étant un identifiant unique du porteur)
- Un point de distribution de la liste de révocation (CDP) valide (adresse d'une CRL dans l'annuaire CPS pour une carte CPS)

Cet UPN sera l'identifiant unique du couple {porteur ; carte CPS} qui sera rattaché à un compte utilisateur du domaine Microsoft (voir Annexes pour la structure exacte des UPNs, ainsi que des exemples de script pour un déploiement dans l'Active Directory).

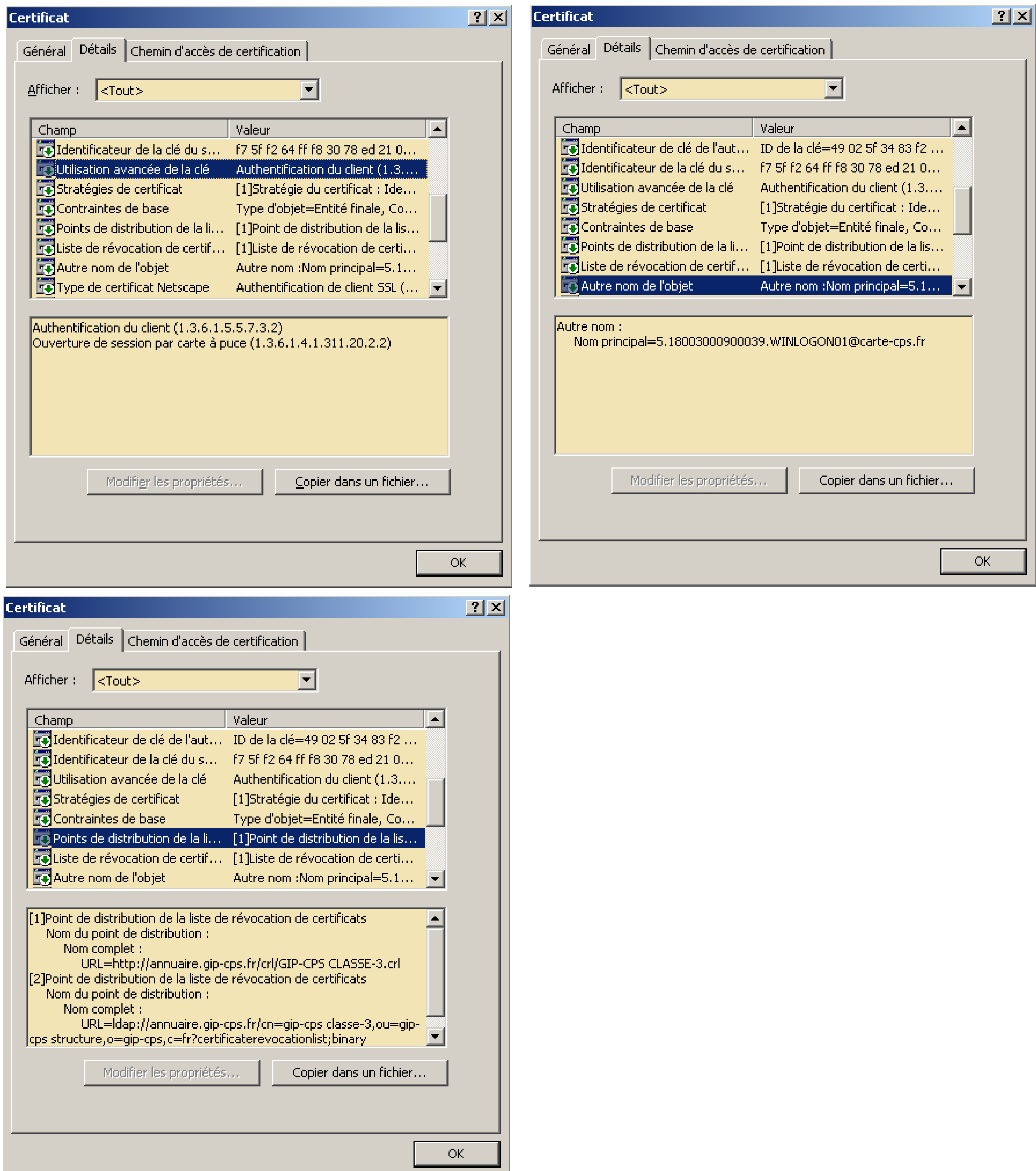
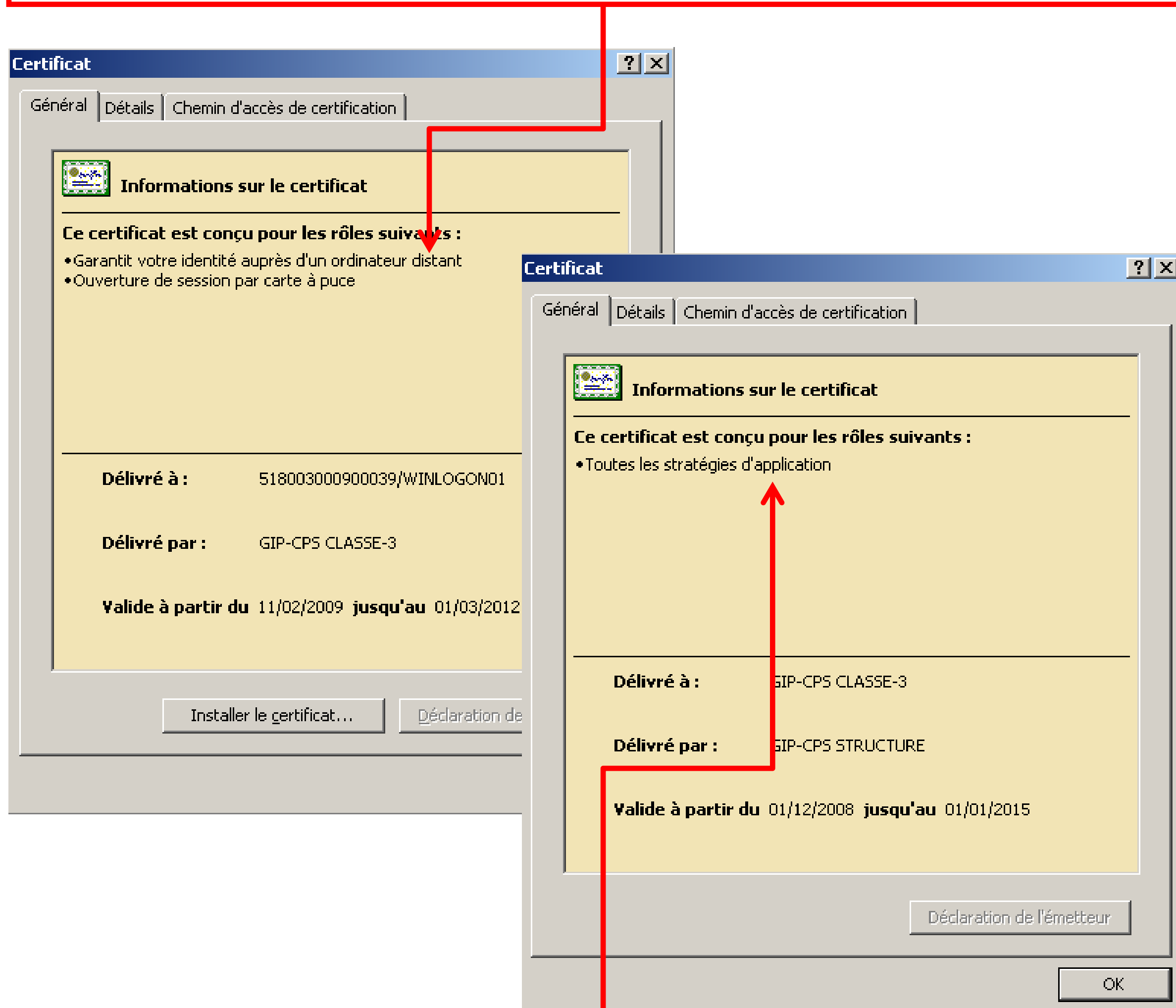


Figure 8 : Exemple d'un certificat de type « Smartcard logon »

Pour qu'un certificat soit utilisable en « ouverture de session par carte à puce » (champ « utilisation avancée de la clé »), il faut qu'il « hérite » de ce rôle: son autorité de certification doit posséder ce rôle dans sa liste des utilisations avancées de la clé.

Exemple d'un affichage correct des rôles d'un certificat « Smartcard logon ». Rôles qui sont autorisés par son autorité de certification (ici GIP-CPS CLASSE-3)



Exemple des rôles de l'autorité de certification (ici GIP-CPS CLASSE-3) d'un certificat « Smartcard logon ».

Figure 9 : Informations des certificats de type « Smartcard logon »

Attention: Cette autorité intermédiaire possédant toutes les stratégies d'application (ExtendedKeyUsage) doit être présente obligatoirement uniquement coté serveur (magasin des autorités intermédiaires et magasin NTAuth).
Coté client, aucune autorité n'est obligatoire (le Winlogon se base uniquement sur le magasin NTAuth alimenté par le serveur)

Remarque: les cartes CPS possédant des certificats compatibles « Smartcard logon » sont diffusées depuis mars 2011 (cartes « CPS3 »).

11Configuration

Cette partie donne les bases pour configurer les différents composants client et serveur décrits précédemment afin de mettre en place et d'administrer le Smartcard logon.

11.1 Configuration du poste client

Cf. Annexe pour des aperçus d'installation du poste de travail.

Les **composants logiciels nécessaires** sur le poste client sont:

- Les Cryptolib CPS v5 de l'ASIP Santé devront être installées
  - Le CSP de l'ASIP Santé, compatible avec le Smartcard logon, devra être installé.
  - Configuration en base de registres du mapping entre l'ATR d'une carte CPS et le CSP ASIP Santé permettant l'accès à la carte CPS.
  - (HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Cryptography/Calais/SmardCards)

La Cryptolib CPS v5 apporte un nouveau CSP faisant abstraction des filières GALSS ou PC/SC : la Cryptolib CPS v5 adresse le lecteur PC/SC nécessaire pour le Smartcard logon directement en PC/SC même si le GALSS est présent.

Le Setup d'installation de cette version de la Cryptolib CPS installe l'ensemble des composants nécessaires au Smartcard logon: PKCS#11, CSP et configuration de la base de registres pour le Smartcard logon.

Il installe aussi l'ensemble des autorités de l'ASIP Santé (racine et intermédiaire) dans le magasin des certificats du poste client (non obligatoire pour l'ouverture de session par carte à puce).

Important : **Sur les postes clients 64 bit, il est nécessaire d'installer les Cryptolib CPS x64**

Une fois l'installation terminée, les erreurs carte à puces disparaissent. Il est alors utile de vérifier le magasin de certificat :

Démarrer > Rechercher Programmes et fichiers > inetcpl.cpl > entrer

En cliquant sur « **Contenu > Certificats** », les magasins apparaissent. Le Magasin « **Personnel** » contient les deux certificats carte d'authentification et de signature.

Il est utile d'identifier le certificat d'authentification et de noter l'UPN associé afin d'enrôler le certificat correctement coté serveur (voir document par ailleurs) :

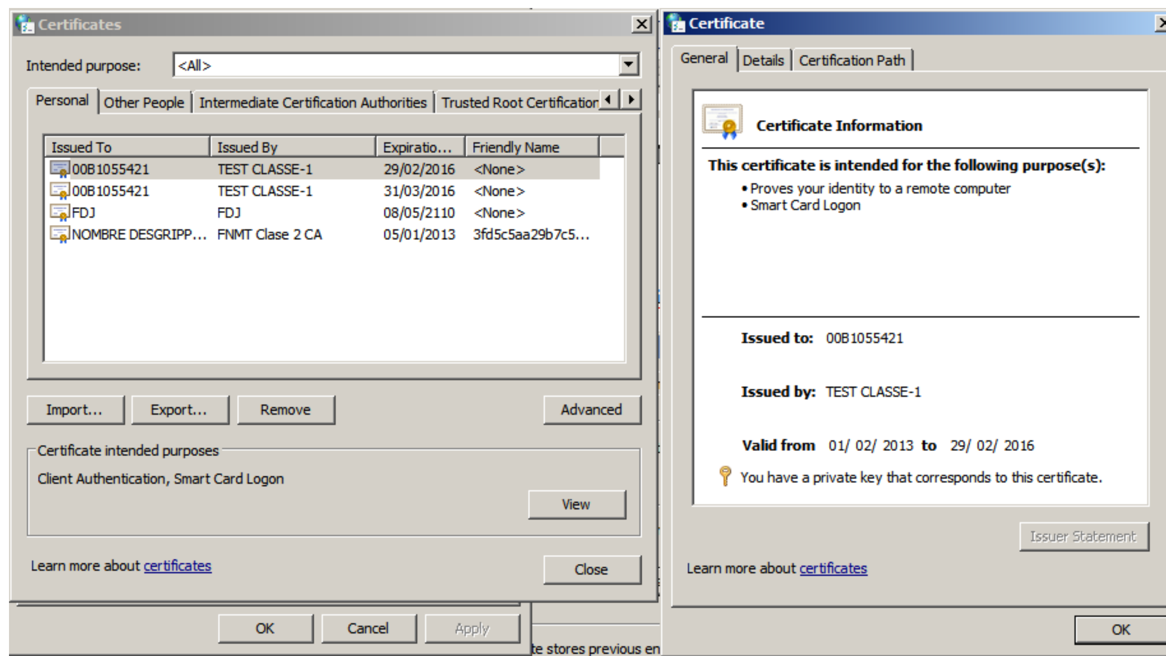


Figure 10 : Poste client: Vérifier le certificat d'authentification

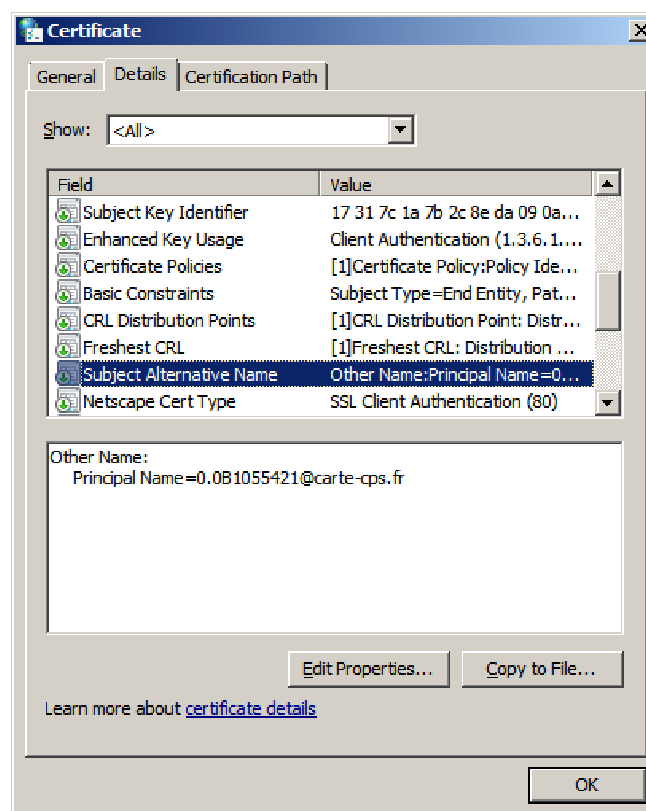


Figure 11 : Poste client: identifier l'UPN du certificat d'authentification

Dans cet exemple, l'UPN est 0.0B1055421@carte-cps.fr.

Cette vérification permet de vérifier les chaines de signatures : les certificats des chaines de certificats concernés par le parc de carte visé devront être correctement provisionnés coté serveur.

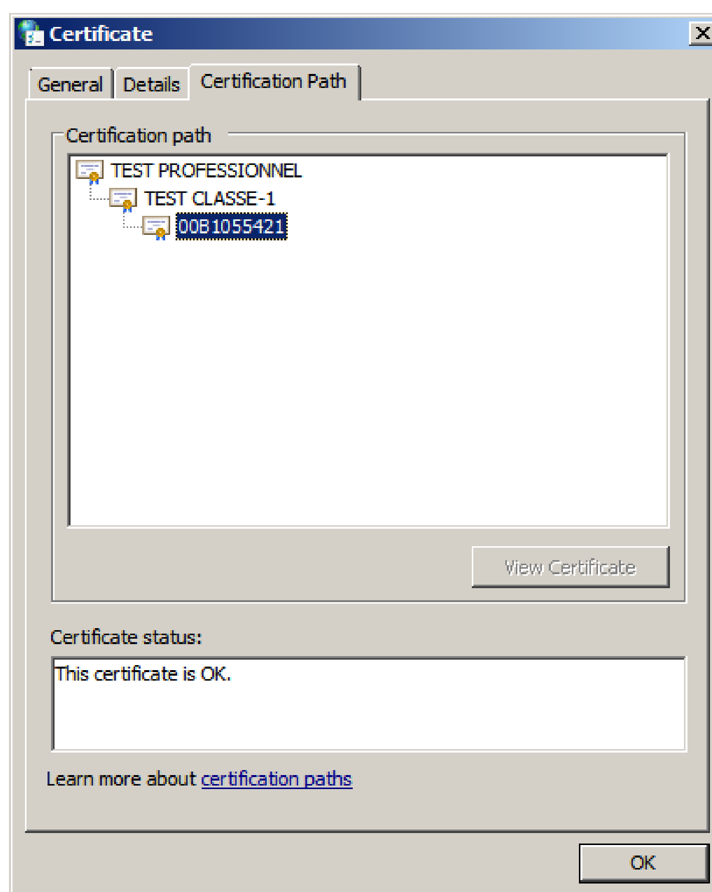


Figure 12 : Poste client: identifier l'UPN du certificat d'authentification

Les certificats d'autorité client (racine et intermédiaire), ainsi que l'autorité racine du serveur, devront être présents dans **le magasin NTAuth** du poste client (propagé exclusivement par le contrôleur de domaine principal (PDC), lors de l'ajout du poste client au domaine, puis régulièrement).

11.2 Configuration Serveur allégée

Cf. Annexe pour des aperçus d'installation d'un serveur Windows 2008R2 Server.

Afin de s'approprier les tâches de paramétrage liées à la configuration de la fonction de Smartcard logon, il est utile d'installer un unique serveur offrant les fonctionnalités suivantes :

- Active Directory (sans DNS, si un DNS est déjà présent sur le réseau local!)
    - **Cf. annexe d'installation d'un rôle Active Directory**
- Certificate Serveur
    - **Cf. annexe d'installation d'un rôle Certificate Server (« AD CS »)**
- Remote desktop (facultatif mais utile)
    - **Cf. annexe d'installation d'un rôle Remote Desktop**
- IIS (facultatif mais utile)
    - **Cf. annexe d'installation d'un rôle IIS**

11.3 Configuration d'un contrôleur de domaine

Cf. Annexe pour des aperçus d'installation d'un serveur Windows 2008R2 Server.

Les postes clients devant être déclarés sur un domaine du réseau, au moins un contrôleur de domaine doit être présent sur le réseau interne.

Les systèmes d'exploitation possibles pour un contrôleur de domaine sont:

- Windows 2003R2 SP1 Server
- Windows 2008R2 SP1 Server
- Windows 2012

Les rôles installés sur le(s) serveur(s) de domaine sont:

- contrôleur de domaine basé sur Active Directory de Microsoft
    - Tout autre annuaire d'identification réseau peut être utilisé, mais la configuration du Smartcard logon sera beaucoup plus complexe

Cf. annexe d'installation d'un rôle Active Directory

Sur le contrôleur primaire (PDC – Primary Domain Controller):

➔ **Ajout des autorités racine** (de confiance) client et serveur à la stratégie de groupe du domaine.
(par interface graphique : Outils d'administration -> Stratégie de sécurité du domaine -> Paramètres de sécurité -> Stratégie de clés publique -> Autorité de certification racines de confiance -> importer)

➔ **Ajout des autorités racine** (de confiance) et intermédiaire au container **NTAuth d'Active Directory**, dans le but de diffuser ces autorités aux machines déclarées sur le domaine (pour permettre une vérification du certificat serveur par les postes client).
En fonction de la version du serveur, cette opération se fera soit par fichiers de script (Windows 2000 Server), soit par interface graphique (à partir de Windows 2003 Server)

Sur chaque contrôleur (primaire et secondaires, si présents):

- ➔ **Installation du provider de révocation de l'ASIP Santé** (pour vérifier que les CRLs correspondant à la chaîne de certification du certificat client sont non révoquées) Ce provider peut être récupéré à l'adresse suivante : http://www.microsoft.com/france/interop/ressources/gip-cps.aspx
- ➔ **Ajout des autorités racine et intermédiaires** dans les différents magasins correspondants (voir le document d'**installation/configuration du provider de révocation de l'ASIP Santé**), pour permettre au provider de révocation de vérifier la validité des CRLs.

Cf. annexe d'installation du provider de révocation ASIP Santé

Cf. annexe de configuration du Contrôleur de domaine (certificats)

Cf. tableau 11 et tableau 12, ci-après, récapitulatifs des étapes d'installation et de configuration dans un scénario d'implémentation de serveur « allégé »

Il est aussi nécessaire de rattacher les comptes utilisateur à leurs cartes CPS respectives.

Dans Active Directory, pour chaque compte utilisateur du domaine, on rajoutera l'**UPN de la carte CPS** associé à ce compte au champ **« nom d'ouverture de session de l'utilisateur »** (une seule carte possible par compte).

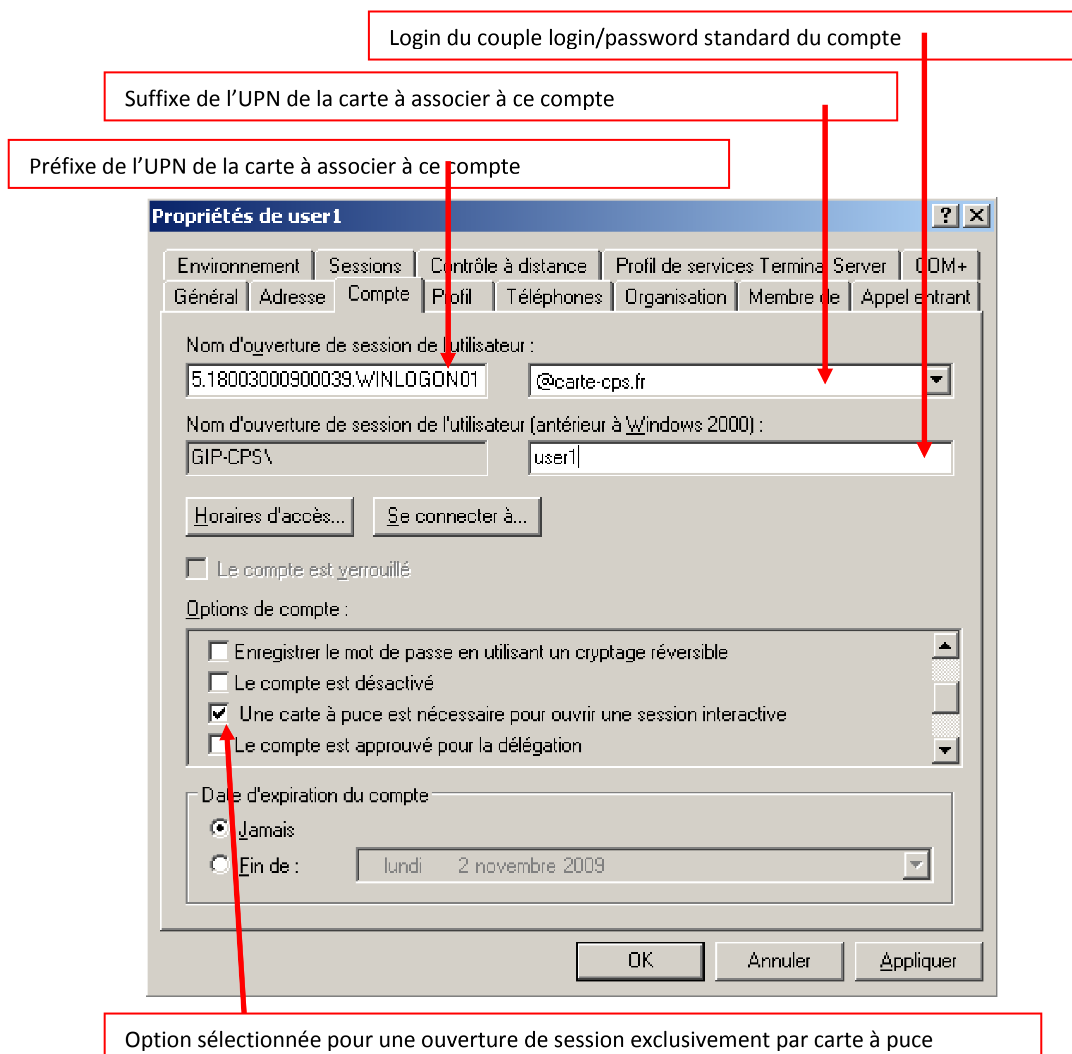


Figure 13 : Active Directory: Smartcard logon : Configuration d'un compte utilisateur

Cf. annexe de configuration du poste de travail (vérification des UPNs)

Cf. annexe de configuration du Contrôleur de domaine (certificats et utilisateur)

Si le suffixe de l'UPN n'apparait pas dans la liste des noms de domaines connus, une relation d'approbation avec le domaine existant devra préalablement être créée:

Outils d'administration -> **Domaines et approbations Active Directory.**

Pour ajouter une approbation au domaine existant :

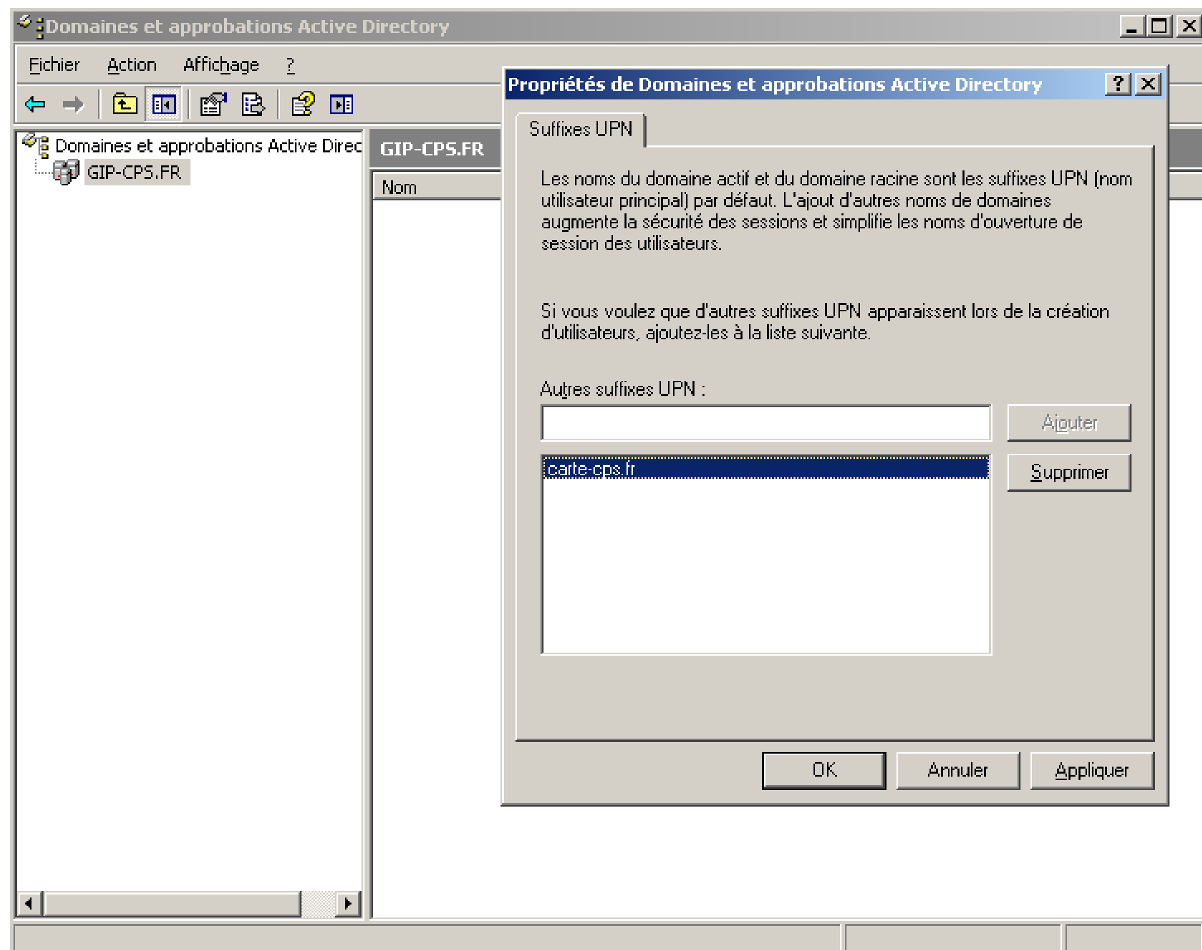


Figure 14 : Active Directory: Approbation du suffixe UPN « carte-cps.fr »

Remarque: le nom de domaine DNS « **carte-cps.fr** » a été réservé par l'ASIP Santé.

11.4 Configuration du serveur de certificats (PKI Microsoft)

Ce chapitre explique comment installer/configurer une PKI Microsoft avec le composant Microsoft Certificate Server.

Certificate Server est un composant gratuit intégré aux versions Server de Windows. Comme expliqué précédemment, il pourra donc être installé sur une machine serveur présente sur le domaine. Il peut être installé directement sur le serveur faisant office de contrôleur de domaine (par exemple, dans le cas d'un petit réseau, qui ne peut pas dédier un serveur à cette tâche uniquement).

Il est cependant préférable pour des raisons :

1. de sécurité
2. de fiabilité du réseau

de l'installer sur une autre machine du domaine, qui sera dédiée à ce rôle.

L'installation de Certificate Server sur un serveur le « gèle »: il est ensuite impossible de modifier son nom ou son domaine tant que ce composant est installé.

Procédure d'installation : « **Panneau de configuration -> Ajout/suppression de programmes -> Ajouter/Supprimer des composants -> Service de certificats (PKI Microsoft)** »

L'installation se déroule automatiquement. Durant cette installation, il sera demandé de générer l'autorité racine de cette PKI :

- **Type d'autorité** : obligatoirement : autorité racine d'entreprise (pour permettre la propagation automatique de cette autorité sur toutes les machines du domaine)
- **Nom commun et période de validité de l'autorité** : à définir en fonction de la politique de sécurité du réseau informatique local.

Cf. annexe d'installation d'un rôle Certificate Server (« AD CS »)

Une fois l'autorité de certification générée et l'installation terminée, cette autorité est automatiquement déployée sur toutes les machines du domaine.

Il ne reste plus ensuite qu'au contrôleur de domaine à faire une demande de certificat serveur de type DC (Domain Controller), auprès de cette autorité.

(Au reboot du contrôleur de domaine : inscription automatique auprès de la PKI du domaine, et demande automatique d'un certificat serveur DC)

Ce serveur hébergeant la PKI devra être en permanence accessible via le réseau par protocole LDAP depuis toutes les autres machines qui veulent vérifier la non-révocation du certificat serveur et depuis son autorité.

11.5 Configuration des options de sécurité

Ce chapitre explique quelques réglages de base du Smartcard logon pour une meilleure sécurité du domaine géré.

11.5.1 Forcer l'utilisation de la carte à puce

Par défaut, un compte configuré pour ouvrir une session par carte à puce, pourra aussi ouvrir une session par login/mot de passe.

Pour augmenter la sécurité du réseau, il sera recommandé d'imposer l'ouverture de session uniquement par carte à puce.

Pour cela, 2 possibilités :

- ⇨ Soit à partir d'un compte utilisateur : sélection de l'attribut « **Carte à puce nécessaire pour ouvrir une session interactive** ». Dans ce cas, le mot de passe du compte utilisateur sera modifié automatiquement à une valeur inconnue.
- ⇨ Soit par stratégie de groupe (**secpol.msc**) : **« Paramètres de sécurité locaux -> Stratégie locale -> Options de sécurité -> Interactive Login : Smart Card Required »**
    - **Valeur : activated**

  Requiert au minimum Windows XP SP2 pour les postes client. Ne modifie pas le mot de passe du/des compte(s) utilisateur impacté(s) par la stratégie.

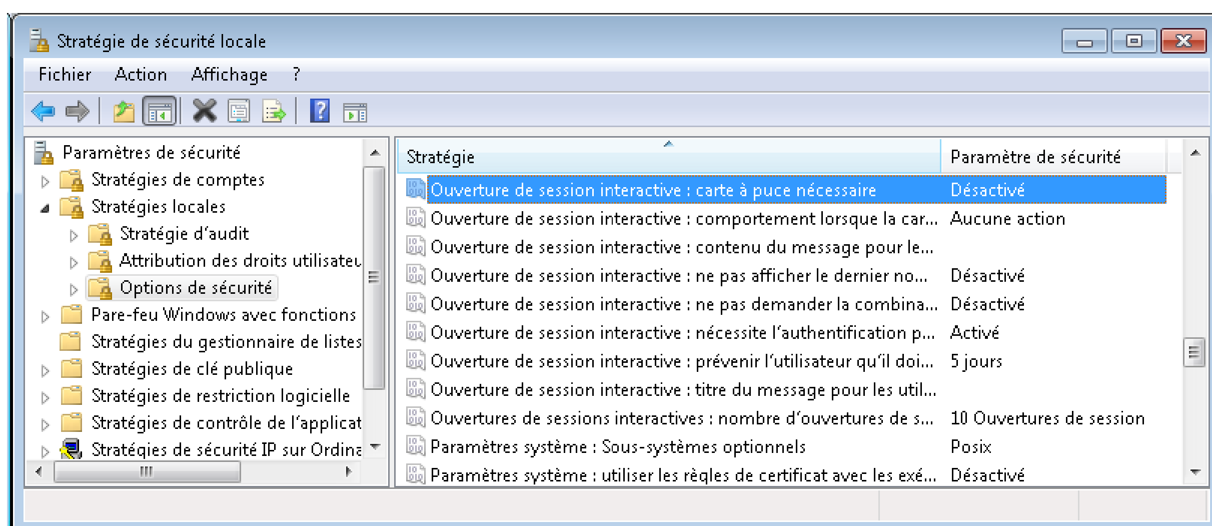


Figure 15 : Forcer l'utilisation de la carte à puce par stratégie locale

Attention: l'utilisation de cette stratégie impacte tous les comptes, dont les comptes administrateurs, qui auront besoin d'une carte à puce pour se logger

11.5.2 Comportement du système au retrait de la carte à puce

Par défaut, à l'extraction de la carte à puce du lecteur pendant une session, aucune action n'est réalisée.

Mais pour plus de sécurité, il est possible de configurer le comportement de la session sur cet évènement d'arrachage de carte :

Par stratégie de groupe : « **Paramètres de sécurité locaux -> Stratégie locale -> Options de sécurité -> Comportement lorsque la carte est retirée »**

- Aucune action.
- Verrouille session (verrouillage de la session).
- Force Logout. (fermeture de la session).

11.5.3 Forcer l'approbation du contrôleur de domaine à l'ouverture de session

Par défaut, si le contrôleur de domaine est injoignable ou indisponible, une session cliente peut être ouverte même sans réponse du serveur, en utilisant les informations de session mises en cache.

Ceci est valable aussi bien en ouverture de session par login/password qu'en ouverture de session par carte à puce.

Les informations de la dernière session ouverte sont alors utilisées, ce pour un certain nombre d'ouvertures de session sans contrôleur de domaine, défini par stratégie de groupe.

Il est possible de modifier ce comportement en forçant l'approbation du serveur de domaine à chaque ouverture de session, par stratégie de groupe :

« Paramètres de sécurité du contrôleur de domaine -> options de sécurité -> ouverture de session interactive -> nécessite l'authentification par le contrôleur de domaine pour le déverrouillage… -> **Activé** »

Attention: dans ce cas, si le serveur est injoignable, la session ne pourra pas s'ouvrir.

11.5.4 Désactivation de la vérification des CRLs

A partir de Windows 2008 server, il est possible de désactiver la vérification des CRLs des certificats carte et serveur et donc de ne pas utiliser de provider de révocation.

Cette option est déconseillée car elle diminue le niveau de sécurité du SI (pas de vérification sur l'état de révocation des cartes utilisées) mais elle peut être utile, par exemple :

1. dans le but de faciliter les tests
2. pour valider des architectures réseau (qui n'ont pas forcement d'accès externes pour la récupération des CRLs)

Voici les clés à ajouter en base de registres, sur le(s) contrôleur(s) de domaine (contenant le KDC):

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters]
Clé : "UseCachedCRLOnlyAndIgnoreRevocationUnknownErrors" = (type:dword) valeur : 1

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kdc]
clé : "UseCachedCRLOnlyAndIgnoreRevocationUnknownErrors" = (type:dword) valeur : 1
```

Tableau 12 : CPSRev : désactivation de la vérification des CRLs

Il suffit de repasser les valeurs des clés à 0 pour réactiver la vérification des CRLs.

Aucun redémarrage du serveur concerné n'est nécessaire pour la prise en compte des modifications.

11.6 Exemple pratique d'une configuration de serveur

Cf. aperçus écran en annexe.

Conseils:

- imprimer ces 2 tableaux
- imprimer les aperçus en annexe
- annoter les impressions papier au fur et à mesure de l'avancement
- faire des impressions d'écrans
- alimenter le dossier d'exploitation

Exemple de procédure de configuration minimale d'un contrôleur de domaine pour une utilisation Smartcard logon:

Installation	Windows 2008 Server		Windows 2003 Server
Provider de révocation	**Installation du provider de révocation** Cf. annexe pour aperçus d'installation et documentation du provider		Identique Windows 2008 Remarque : le journal CPSRev se trouve directement dans l'observateur d'événements.
	1	Lancement de l'installeur CPSRevSetup.msi	
	2	configuration de la base de registres	
	3	configuration des magasins de certificats	
	4	En cas de contrôleurs de domaine multiple : installation sur chaque contrôleur	
	5	Accès internet requis pour récupération des CRLs	
	Vérification		
	1	Journal « CPSRev » installé dans l'observateur d'événements »-> « journaux des applications et des services »	
	2	commande **certutil -verify cert.cer**	
	3	commande **certutil -pulse** (cert.cer = certificat d'authentification d'une carte CPS)	
Service de certificats (IGC Microsoft)	**Installation de AD CS sur le contrôleur de domaine, ou sur un autre serveur du domaine.** Cf. annexe pour aperçus d'installation		Identique Windows 2008
	1	Gestionnaire de serveur-> Rôles -> Ajouter des rôles -> Service de certificats Active Directory (PKI Microsoft)	
	2	Génération du certificat racine (choisir « **autorité racine d'entreprise** »)	
	3	génération du certificat serveur DC. (généré automatiquement lors de l'installation de la PKI, sur tous les contrôleurs de domaine du domaine)	
	4	Reboot du serveur + contrôleur(s) de domaine.	

Tableau 13 : Serveur: Installation du serveur

<table>
<tr><th>Configuration</th><th colspan="2">Windows 2008 Server</th><th>Windows 2003 Server</th></tr>
<tr><td rowspan="2">Configuration de la stratégie de groupe du domaine.</td><td colspan="2">Ajout des autorités racines client et serveur à la stratégie de groupe du domaine

Cf. annexe pour aperçus de configuration</td><td rowspan="2">Ajout des autorités racines client et serveur :

=> Outils d’administration -> Stratégie de sécurité du domaine -> paramètres de sécurité -> Stratégie de clés publique -> Autorité de certification racine de confiance -> importer</td></tr>
<tr><td colspan="2">commande MMC -> Stratégie Default Domain Controllers policy -> Configuration ordinateur -> paramètres Windows -> Paramètres de sécurité -> Stratégie de clés publique -> Autorité de certification racines de confiance -> importer.</td></tr>
<tr><td rowspan="4">Configuration du container NTAuth (Active Directory)</td><td colspan="2">Ajout des certificats d’autorités client (racine + intermédiaire) + serveur (racine) dans le magasin NTAuth.

Cf. annexe pour aperçus de configuration</td><td rowspan="4">Identique Windows 2008
installation préalable de Rktools
pour Windows 2003, pour avoir
le module PKIView (enterprise PKI)</td></tr>
<tr><td colspan="2">commande MMC -> PKI d’entreprise -> gérer les conteneurs Active Directory -> Conteneur NTAuthCertificates -> Ajouter</td></tr>
<tr><td colspan="2">Vérification</td></tr>
<tr><td colspan="2">commande Certutil -viewstore -enterprise NTAuth</td></tr>
<tr><td rowspan="7">Configuration des magasins de certificats du serveur.</td><td colspan="2">Configuration des magasins de certificats du serveur

Cf. annexe pour aperçus de configuration</td><td rowspan="7">Identique Windows 2008</td></tr>
<tr><td colspan="2">Commande MMC -> certificats -> ordinateur local</td></tr>
<tr><td>Magasin Personnel</td><td>certificats racine ASIP
certificat du contrôleur de domaine émis par l’AD CS</td></tr>
<tr><td>Magasin Autorités de certification racine de confiance</td><td>certificats racine ASIP
certificat du contrôleur de domaine émis par l’AD CS</td></tr>
<tr><td rowspan="2">Magasin Autorités intermédiaires</td><td>certificats client racine (signeur de CRL)</td></tr>
<tr><td>certificats intermédiaires :
client signeur de certificats et CRLs</td></tr>
<tr><td colspan="2">en cas de contrôleurs de domaine multiple :
installer ces certificats sur chaque contrôleur</td></tr>
</table>

<table>
<tr><th>Configuration</th><th colspan="2">Windows 2008 Server</th><th>Windows 2003 Server</th></tr>
<tr><td rowspan="3">Création d’une relation d’approbation pour le suffixe UPN des cartes CPS.</td><td colspan="2">Ajouter dans la liste le suffixe de l’UPN de la carte CPS</td><td rowspan="3">Identique Windows 2008</td></tr>
<tr><td>1</td><td>Outils d’administration -> Domaine et approbations AD -> Clic Droit -> Propriétés -> Suffixes UPN</td></tr>
<tr><td>2</td><td>Ajouter dans la liste le suffixe de l’UPN de la carte CPS. (« carte-cps.fr » pour les cartes CPS compatible Smartcard logon)</td></tr>
<tr><td rowspan="5">Configuration d’un compte utilisateur sur Active Directory</td><td colspan="2">Attacher l’identifiant de la carte CPS (l’UPN présent dans le certificat d’authentification de la carte CPS) à un compte utilisateur Active Directory</td><td rowspan="5">Identique Windows 2008</td></tr>
<tr><td>1</td><td>Ouvrir les propriétés d’un compte utilisateur du domaine.</td></tr>
<tr><td>2</td><td>Onglet Compte : dans le champ « nom d’ouverture de session de l’utilisateur » : ajouter l’UPN de la carte à associer à ce compte.</td></tr>
<tr><td colspan="2">Vérification</td></tr>
<tr><td colspan="2">le suffixe de l’UPN, créé auparavant par relation d’approbation, apparaît dans la liste des suffixes</td></tr>
<tr><td rowspan="4">Test de la configuration</td><td colspan="2">Test de la configuration</td><td rowspan="4">Identique Windows 2008
=> commande Dsstore -pulse au lieu de certutil -pulse

installer Dsstore pour Windows
2003</td></tr>
<tr><td>1</td><td>Configuration poste client minimal : un lecteur PC/SC + son driver + Cryptolib CPS v5</td></tr>
<tr><td>2</td><td>Exécuter sur le contrôleur de domaine : certutil -pulse pour propager les autorités et stratégies sur les postes clients.</td></tr>
<tr><td>3</td><td>Redémarrer une machine cliente, et tester l’ouverture de session par carte CPS.</td></tr>
</table>

Tableau 14 : Serveur: Configuration

11.7 Exemples d’architecture réseau

Exemple d’une architecture réseau « évoluée » : un client sur un domaine A, se connecte à distance sur un domaine B via un canal VPN sur un serveur TSE (ou CITRIX), via une carte CPS.

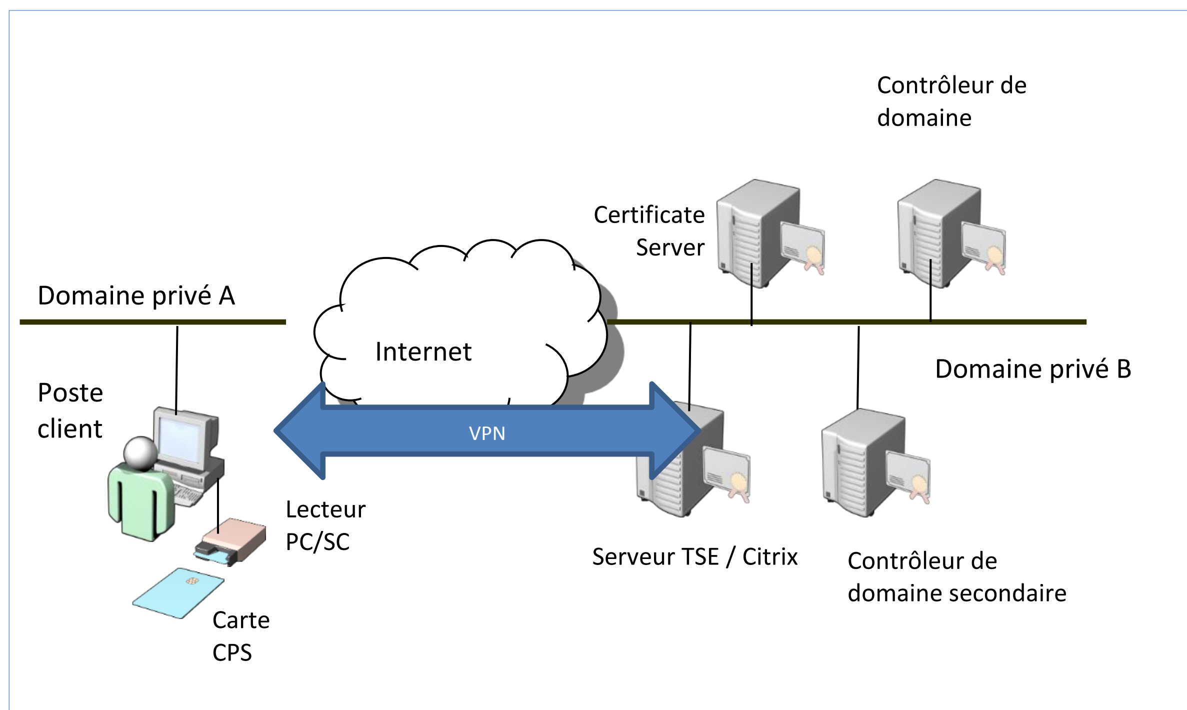


Figure 16 : Architecture : Exemple d’architecture réseau évoluée

12Annexes

Ces annexes présentent la mise en œuvre simplifiée du Smartcard logon avec une carte CPx (maquette).

Cette maquette a pour principaux intérêts :

1. de démontrer la configuration de tous les éléments nécessaires au Smartcard logon avec une carte CPx
2. de le prendre en mains complètement
3. de déterminer s'il correspond ou non aux besoins effectifs de l'entreprise.

L'entreprise pourra à cette occasion en profiter pour faire un bilan

1. de son SI
2. de son référentiel documentaire
3. de ses compétences/connaissances internes relatives aux cartes de santé, à la sécurité et à la PKI

12.1 Maquette de Smartcard logon avec une carte CPx

12.1.1 « Brief Project »

Clé	Valeur	
Nom	Projet « maquette » de Smartcard logon avec une carte CPx	
Objectifs	**1**	Prendre en main le Smartcard logon
	2	Mesurer la pertinence du cas d'usage dans le contexte particulier de l'entreprise
	3	Affiner l'expression de besoin
	4	Tester les réactions utilisateurs
	5	Tirer un bilan sur l'état du SI : états des DEX / DAT / PCA, adéquation des niveaux de sécurité requis vs. Implémentés, bilan des flux
	6	Monter en compétence les équipes sur la PKI Microsoft et les composants matériels et logiciels ASIP Santé

Tableau 15 : « Brief Project » « maquette de Smartcard logon avec une carte CPx »

12.1.2 Ressources nécessaires

Ressource	Rôle	Profil	Implication
MANAGEMENT_1	Donne son aval au projet	DSI / RSSI	0,5 jours
PROJET_1	Collecte les différents documents d'architecture existants Prend connaissance du guide Ecrit l'expression de besoin Ecrit le scénario de démonstration Veille aux jalons Assure la cohérence des tests Organise la démonstration Met à jour les documents d'architecture existants Ecrit et rapporte le « project learning »	Chef de projet	7,0 jours
INTEG_CLIENT_1	Installe et configure 1 ou 2 postes clients, reflet des postes de travail de l'entreprise Teste unitairement ses installations.	Technicien poste de travail Windows connaissant le poste de travail Santé&Social	2,0 jours
INTEG_SERVER_1	Installe et configure la partie serveur. Teste unitairement ses installations.	Ingénieur Système pré sensibilisé à la PKI.	6,0 jours
DEVEL_SERVER_1	En fonction de l'expression de besoin, automatise les tâches d'édition de l'annuaire de l'entreprise pour l'adapter au Smartcard logon. A défaut : identifie et documente les développements nécessaires. Teste unitairement ses développements.	Ingénieur développement idéalement C#/PowerShell connaissant Active Directory et LDAP	3,0 jours
QA_1	Ecrit le plan de test fonctionnel Passe le plan de test Donne son aval pour la démonstration (qualité suffisante, adéquation avec l'expression de besoin).	Testeur connaissant les usages poste de travail Santé&Social	2,0 jours

Tableau 16 : Ressources « maquette de Smartcard logon avec une carte CPx »

12.1.3 Livrables

#	Livrable	Responsable
1	Expression de besoins	PROJET_1
2	Spécifications / Scénario de démo	PROJET_1
3	Cahier de tests unitaires DEV	INTEG_SERVER_1
4	Cahier de tests « Assurance Qualité » (« QA »)	QA_1
5	Maquette	PROJET_1
6	Dossier d'Architecture Technique (DAT) Maquette (config. Poste de travail utilisé, versions de composants serveurs et client, flux, IP, …)	PROJET_1
7	Spécifications des développements réalisés ou à réaliser	DEVEL_SERVER_1
8	Analyse de gaps sur les documents suivants : • Dossier d'Architecture Technique (DAT) • Dossier d'exploitation (DEX) • Plan de Continuité d'Activité (PCA)	PROJET_1
9	Bilan projet (avec Pros&Cons, limitations identifiées documentées, besoins en développements identifiés et évalués)	PROJET_1

Tableau 17 : Livrables « maquette de Smartcard logon avec une carte CPx »

12.1.4 Macro-Planning

Jalon	Description	Valeur
T0	Date de début	(ici 10/02/2014)
T1	Début de l'intégration (Spécifications et cahiers de tests validés)	T0 + 7j
T2	Début des tests « Assurance Qualité » (Q&A)	T0 + 15j
T3	Début Démo et project learning	T0 + 17j
T4	Date de fin	T0 + 20j

Tableau 18 : Macro-planning « maquette de Smartcard logon avec une carte CPx »

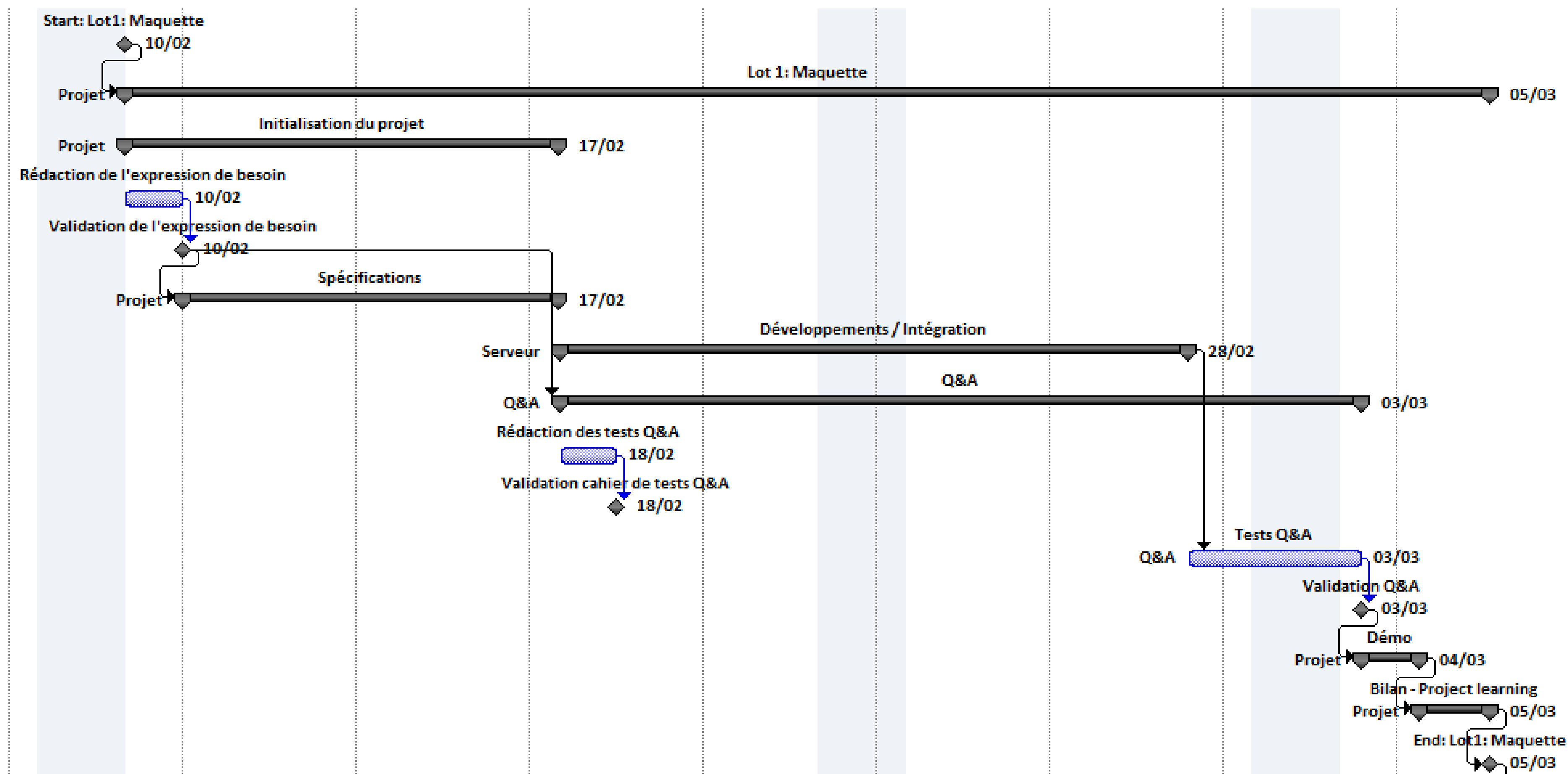


Figure 17 : Macro-planning « maquette de Smartcard logon avec une carte CPx »

12.1.5 Remarques

#	Remarques
1	**Ces éléments sont donnés à titre indicatif**. Ils correspondent aux retours d'expérience de l'ASIP Santé sur le sujet. Ils sont fournis pour aider à la décision et pour éviter les déconvenues. **Ils n'engagent en aucune manière l'ASIP Santé quant à la réussite du projet (techniquement, en coûts ou en délais)**. Chacun verra, au final, midi à sa porte afin de mener à bien ce projet.
2	1. Le temps passé en spécification 2. La charge de travail du chef de projet Sont proportionnellement plus importants que sur un projet d'intégration classique du fait de la nature du projet et de ses objectifs : • bilan de l'existant • organisation de la démo en elle-même et project learning o i.e. composition des pièces qui alimenteront le projet définitif
3	La charge de travail de chacun peut augmenter ou diminuer en fonction des profils finalement retenus.
4	Les rôles peuvent être confondus (ex. PROJET_1 et INTEG_SERVER_1, ou INTEG_SERVER_1, DEVEL_SERVER_1 et INTEG_CLIENT_1). Il est cependant recommandé de garder un testeur (QA_1) indépendant, afin de garantir la qualité du démonstrateur et l'intérêt pour le management d'assister à la démo (prise de décision possible).
5	S'agissant d'une maquette, les durées indiquées incluent la recherche de machines physiques disponibles pour la maquette mais n'incluent pas les temps passés en recherche de licences ou en passage de commandes par exemple. Aucun temps de VSR/VABF, aucune tâche de support, aucune re-livraison ne sont inclus.
6	La suite du document détaille les étapes de configuration à effectuer

Tableau 19 : Remarques « maquette de Smartcard logon avec une carte CPx »

12.2 Installation du poste de travail client

Lorsque les Cryptolib CPS ne sont pas installées sur le poste client, les fenêtres de login signalent une erreur de carte à puce:

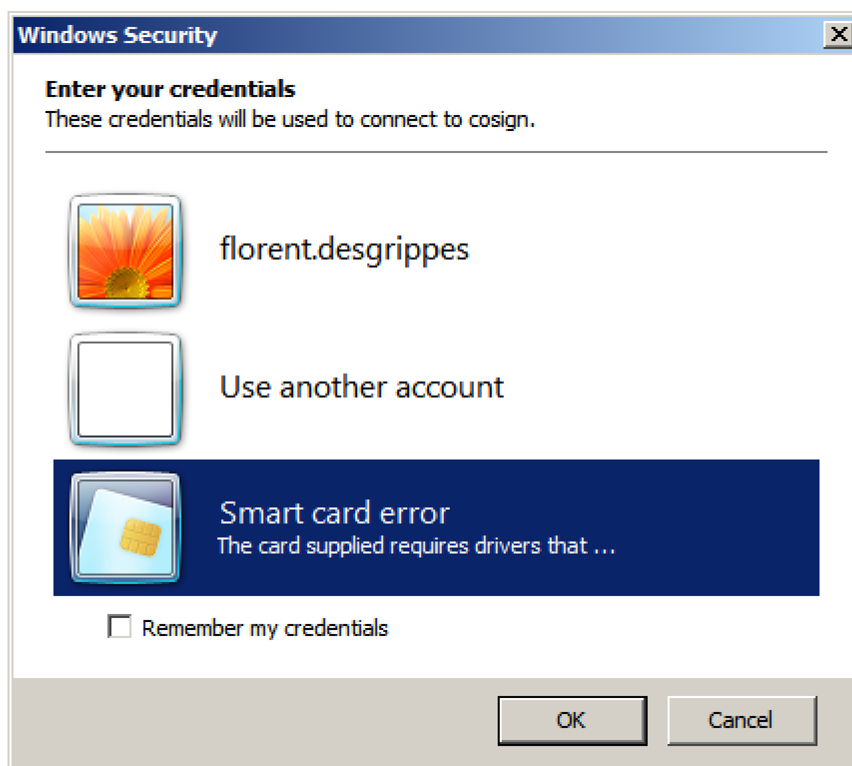


Figure 18 : Poste client : Erreur de carte à puce sur un login TSE si les Cryptolib CPS ne sont pas installées

Important : Seule la version Full PC/SC de la Cryptolib CPS v4 permettait de gérer le Smartcard logon avec des cartes CPS. La Cryptolib CPS v5 apporte un nouveau CSP faisant abstraction des filières GALSS ou PC/SC : la Cryptolib CPS v5 adresse le lecteur PC/SC nécessaire pour le Smartcard logon directement en PC/SC, sans passer par le GALSS. L'insertion de la carte CPS dans un lecteur de type PC/SC reste requis (pas de drivers PC/SC, requis, pour les lecteurs PSS).

Important : Sur les postes clients 64 bit, il est nécessaire d'installer les Cryptolib CPS x64

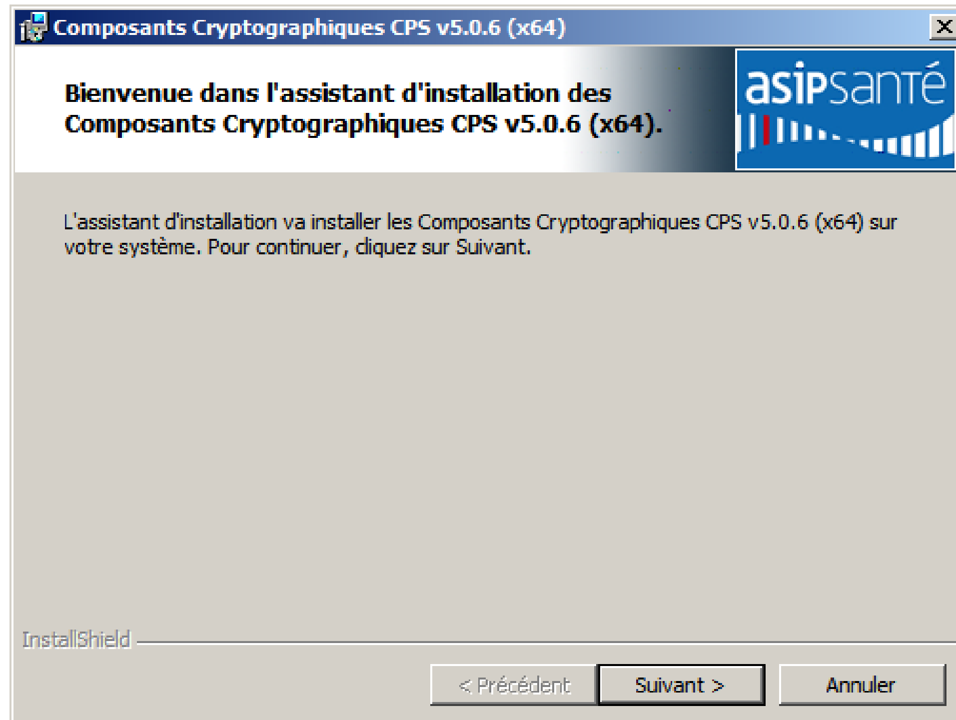


Figure 19 : Poste client : Installation Cryptolib CPS x64

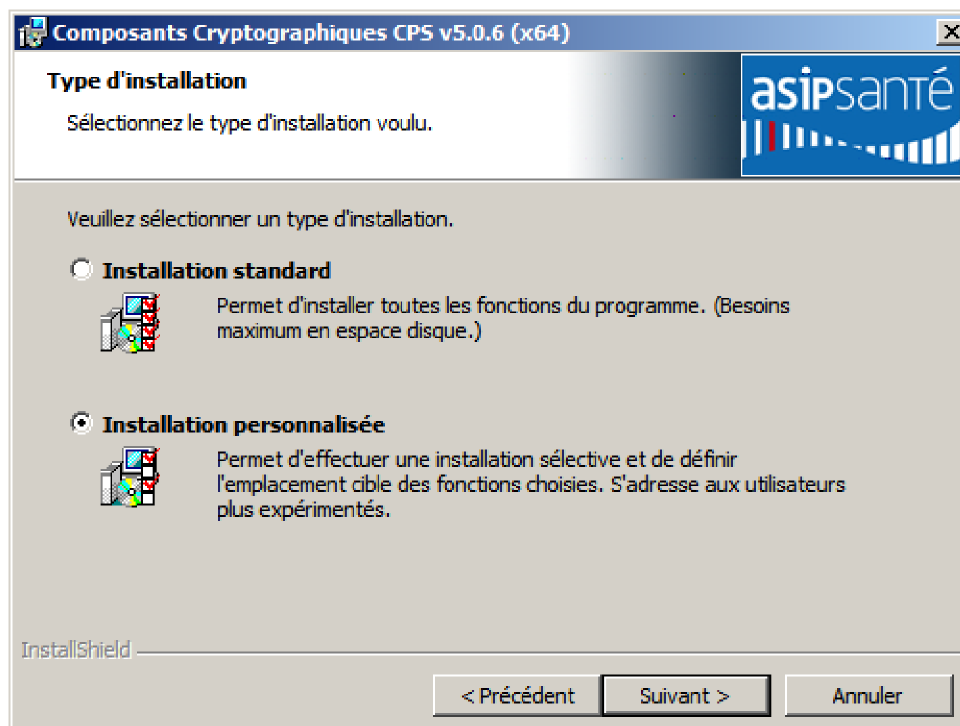


Figure 20 : Poste client: Installation Cryptolib CPS x64 : installation perso avec la filière CPS2Ter Full PC/SC

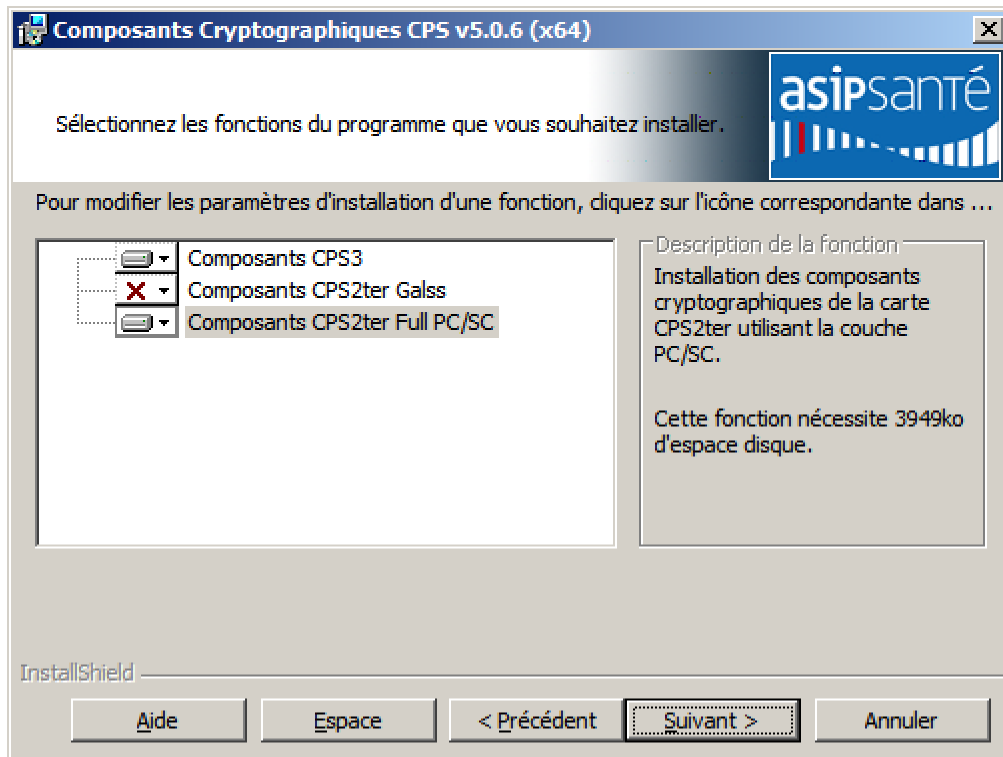


Figure 21 : Poste client: Installation Cryptolib CPS x64 : installation perso avec la filière CPS2Ter Full PC/SC

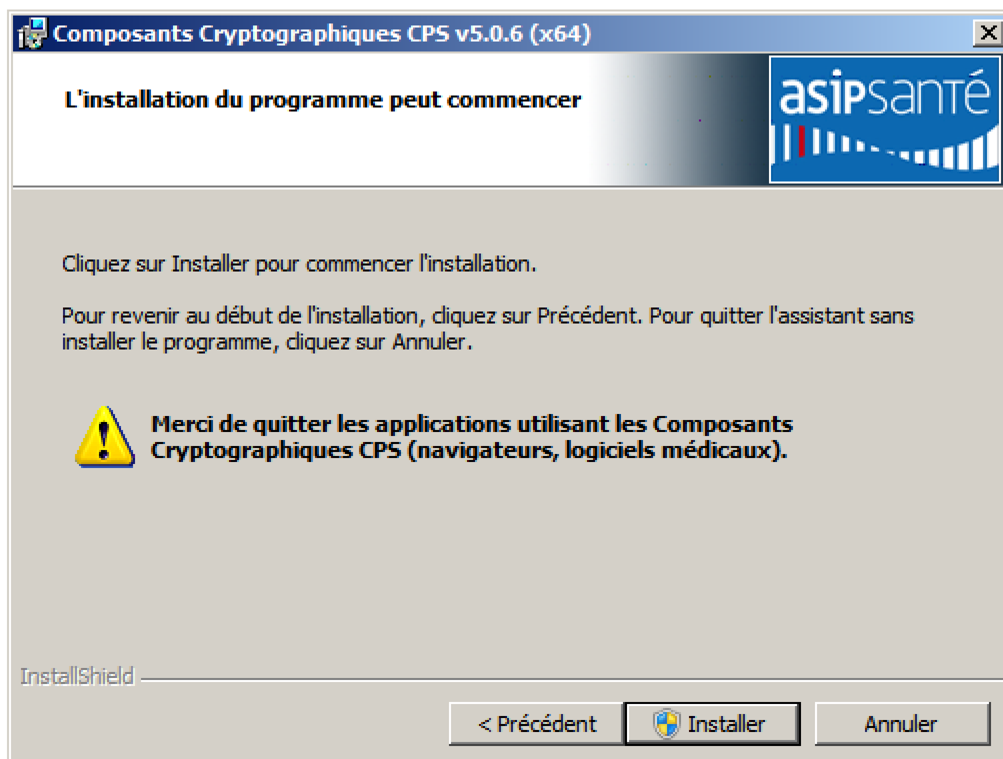


Figure 22 : Poste client : Installation Cryptolib CPS x64 : Installer

Si l'UAC est activée sur le poste, il faut accepter l'installation du MSI fourni par l'ASIP Santé :

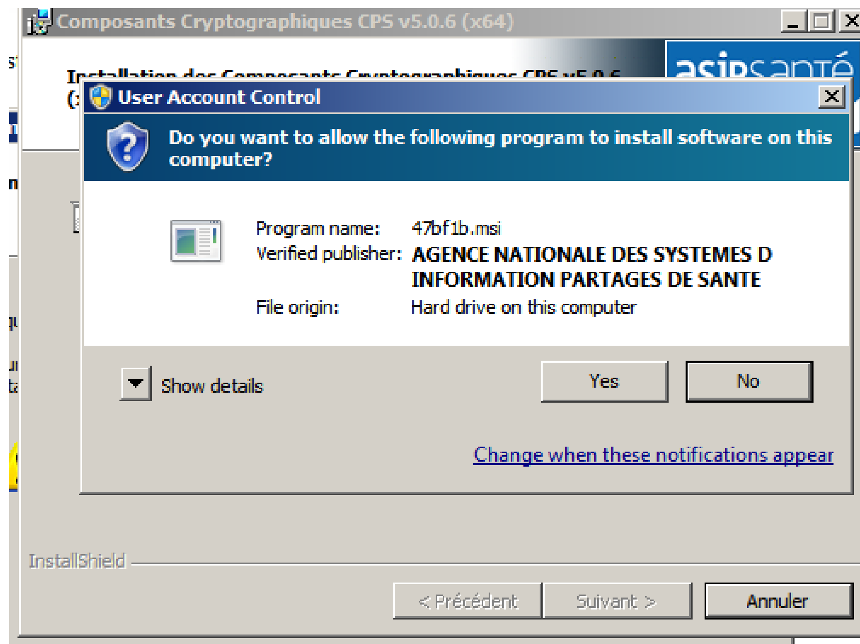


Figure 23 : Poste client: Installation Cryptolib CPS x64 : Fenêtre d'UAC

Certains antivirus peuvent nécessiter des acquittements :

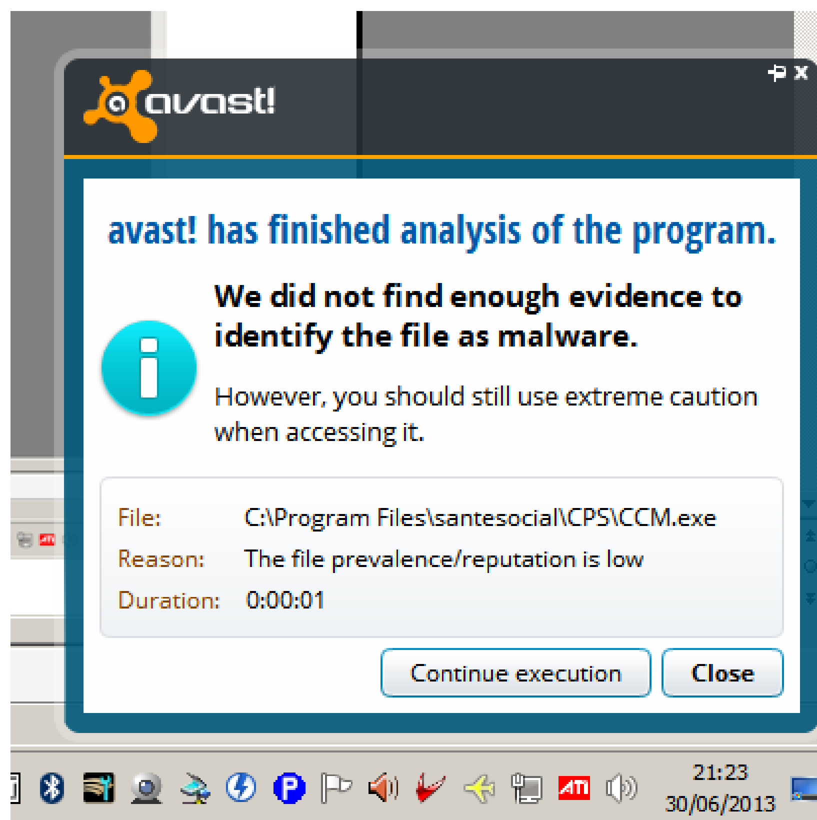


Figure 24 : Poste client : Installation Cryptolib CPS x64 avec AVAST

Une fois l'installation terminée, les erreurs carte à puces disparaissent :

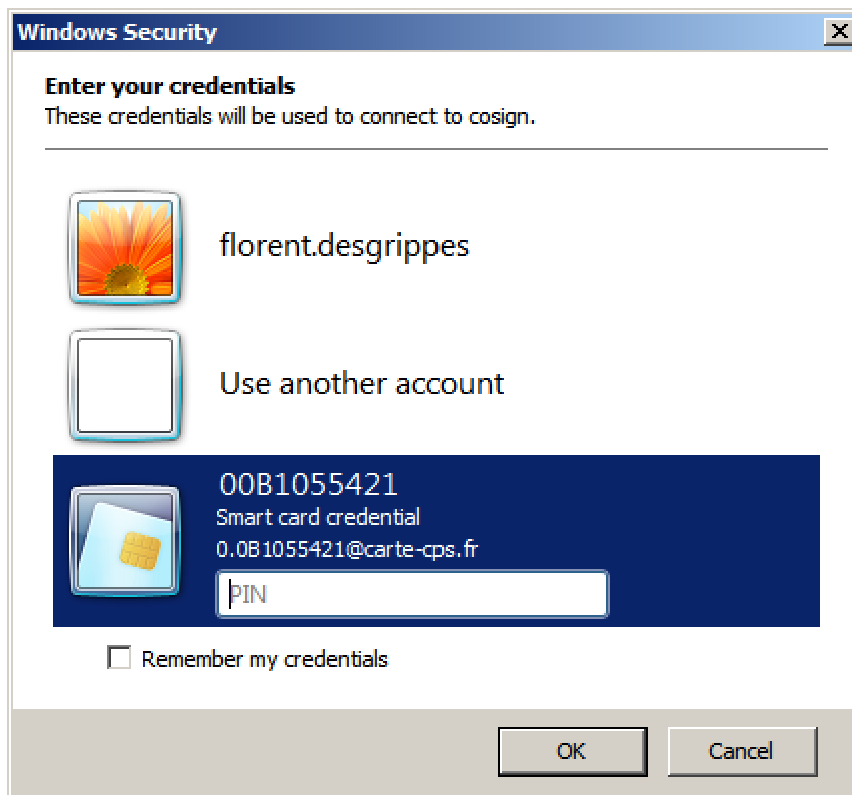


Figure 25 : Poste client : Driver carte à puce OK sur un login TSE (les Cryptolib CPS sont installées)

Vérifier le magasin de certificat :

« **Démarrer > Rechercher Programmes et fichiers > inetcpl.cpl > entrer** »

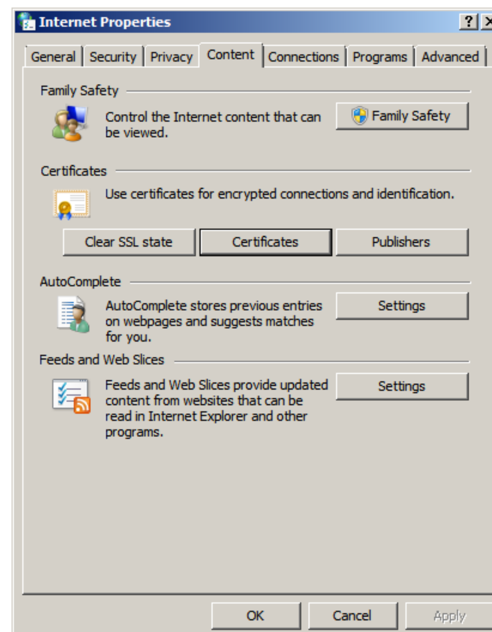


Figure 26 : Poste client : Vérifier le magasin de certificats

Identifier le certificat d'authentification et noter l'UPN

« Contenu > Certificats > Magasin Personnel »

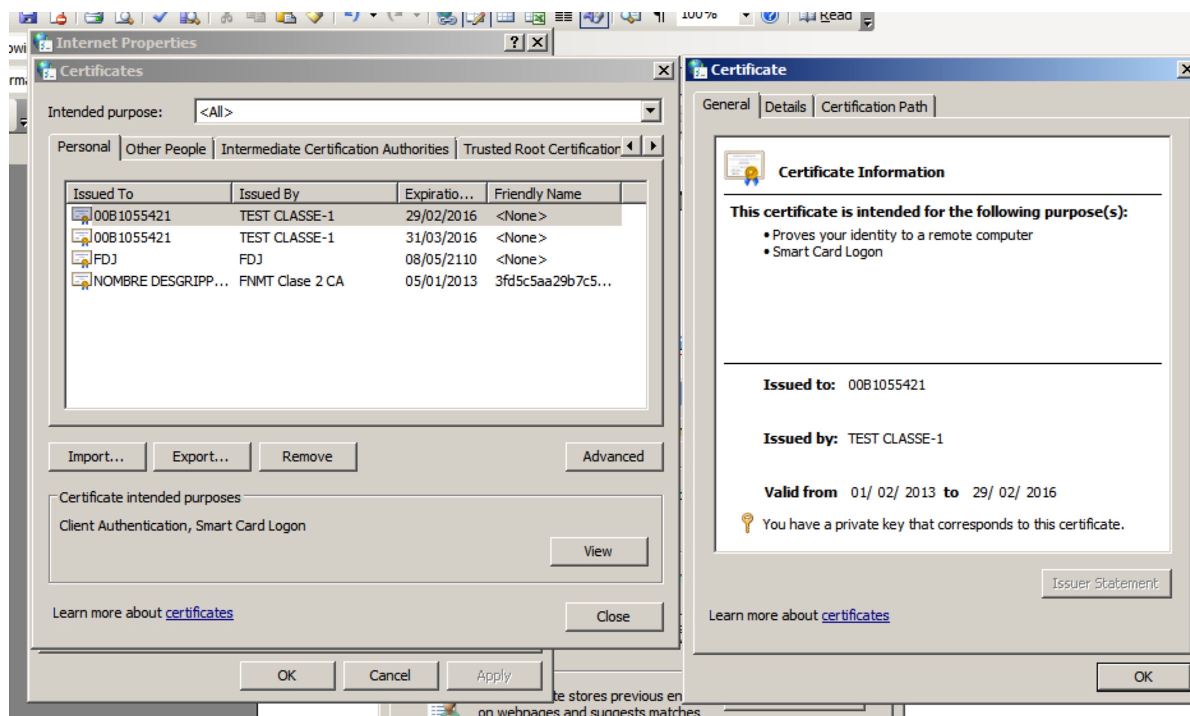


Figure 27 : Poste client : Vérifier le certificat d'authentification

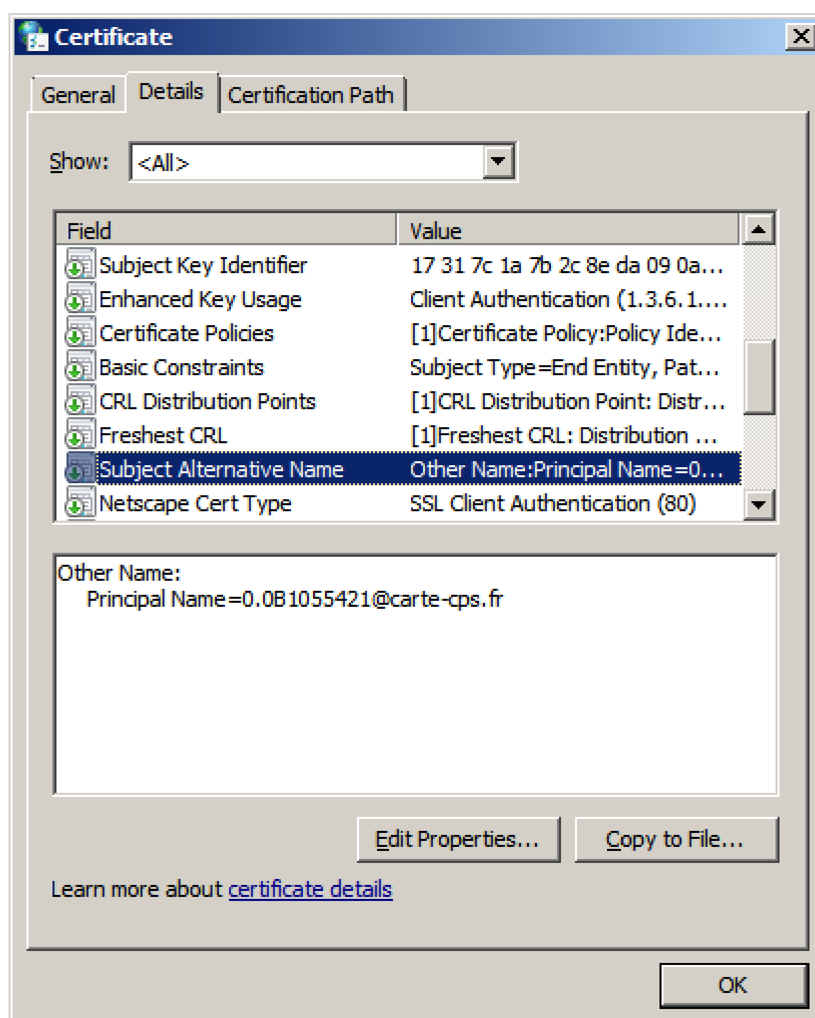


Figure 28 : Poste client : identifier l'UPN du certificat d'authentification

Dans cet exemple, l'UPN est 0.0B1055421@carte-cps.fr.

Vérifier les chaines de signatures : les certificats des chaines de certificats concernés par le parc de carte visé devront être correctement provisionnés coté serveur.

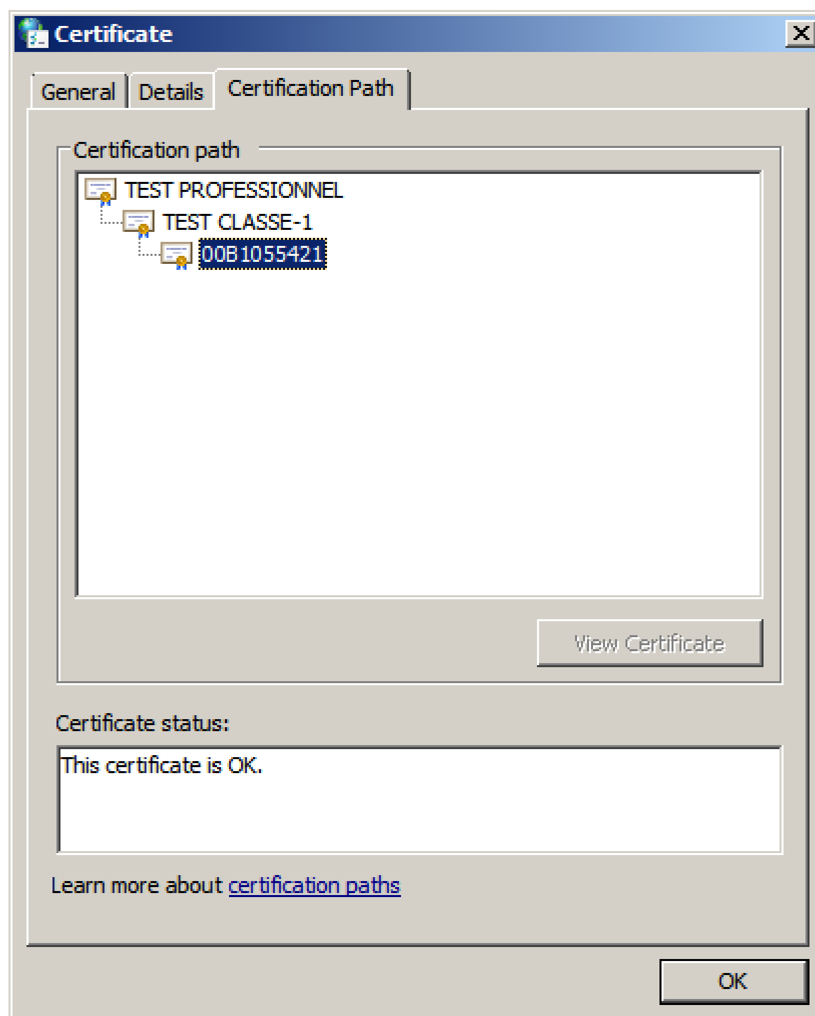


Figure 29 : Poste client : identifier l'UPN du certificat d'authentification

Conseil : pour les postes clients Win7 d'un parc, il est conseillé de

1. désactiver la rechercher automatique de drivers de cartes à puces
2. de maitriser la politique de mises à jour Windows Update des postes

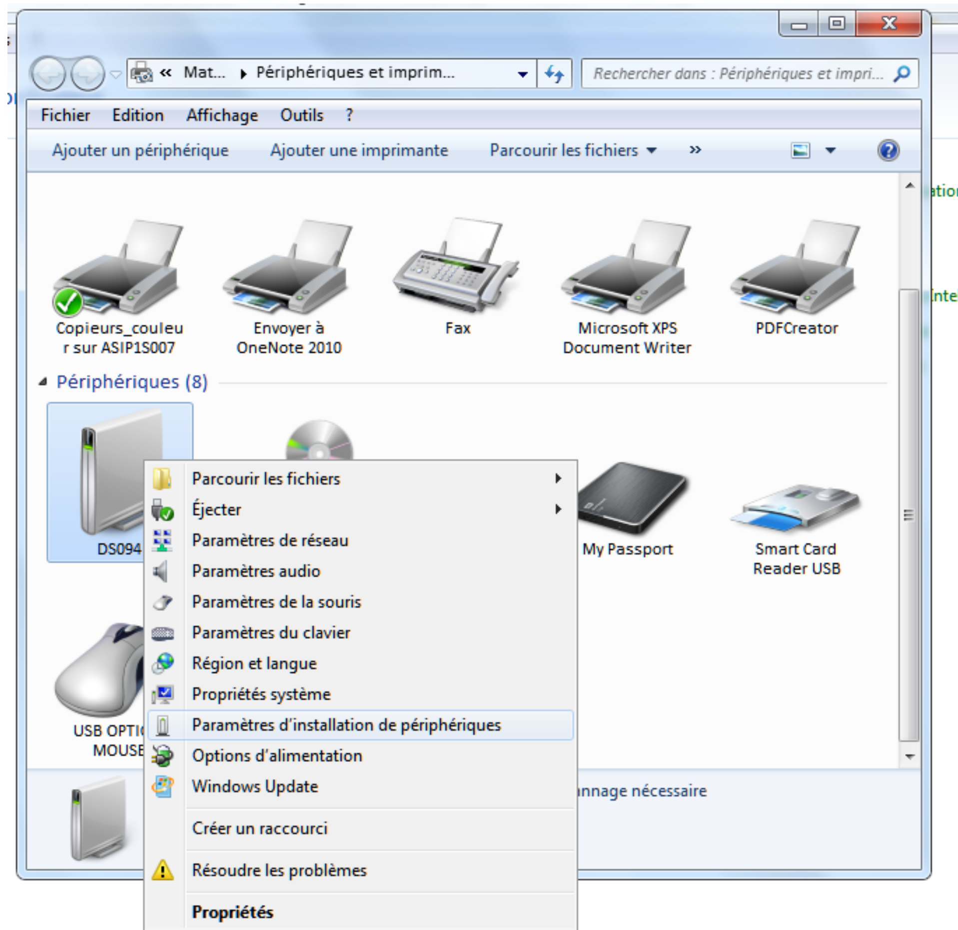


Figure 30 : Poste client : Périphériques et imprimantes : Paramètres d'installation de périphériques et Windows Update

12.3 Installation de Windows 2008 R2 SP1

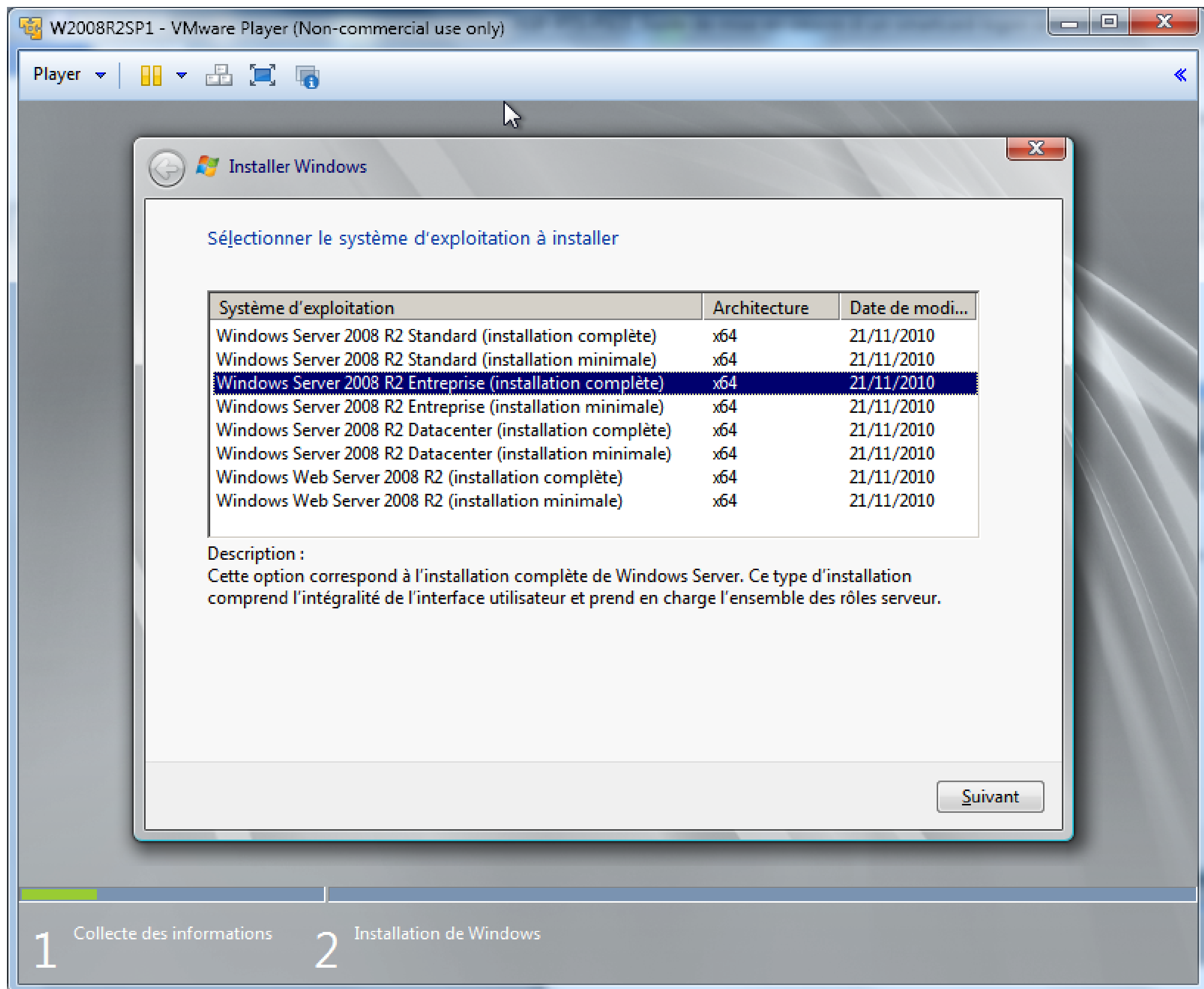


Figure 31 : Windows serveur: Installation: choix du type d'installation

Choisir Windows 2008R2 SP1 (64bit) Enterprise Full

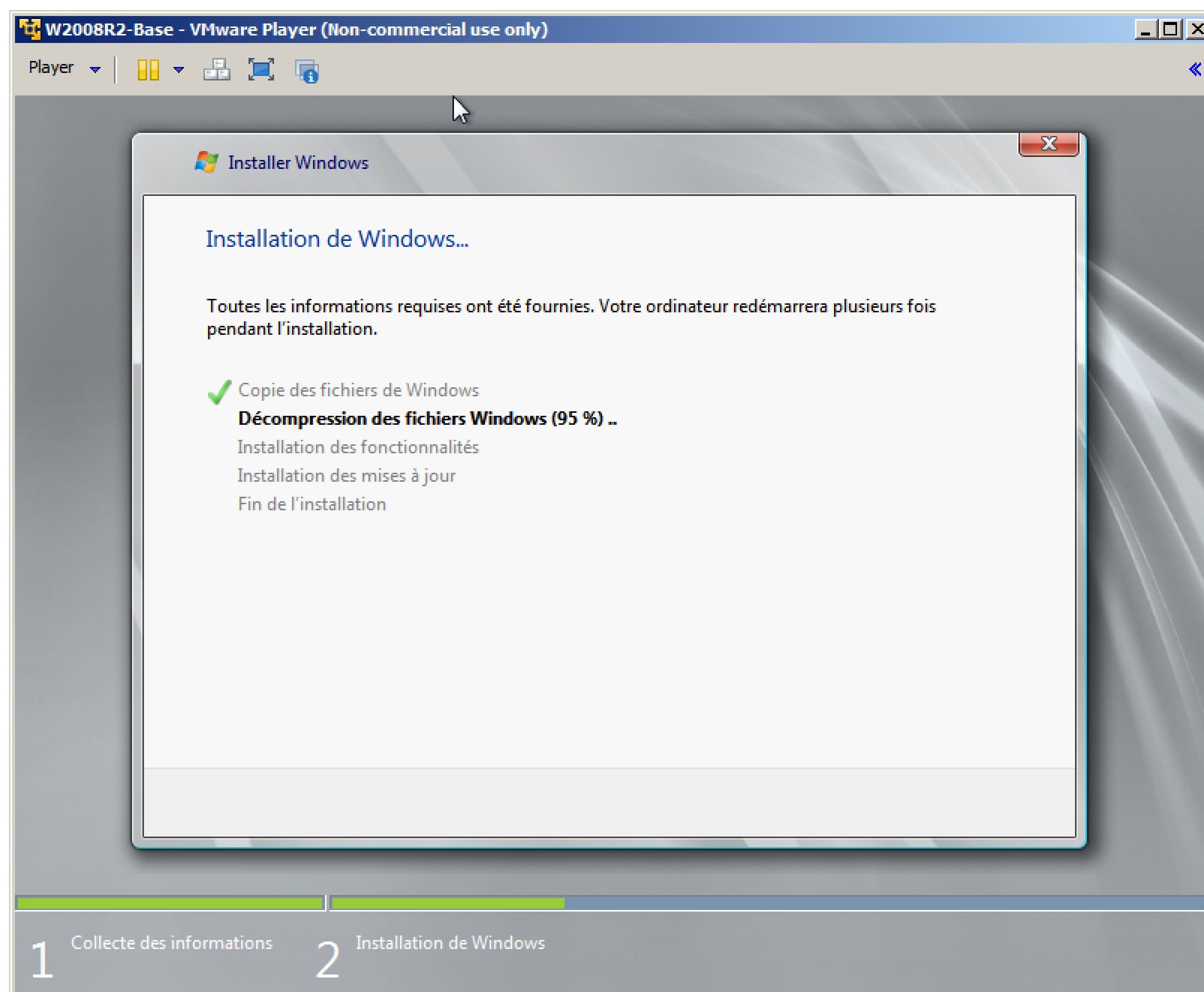


Figure 32 : Windows serveur: Installation: copie de fichier

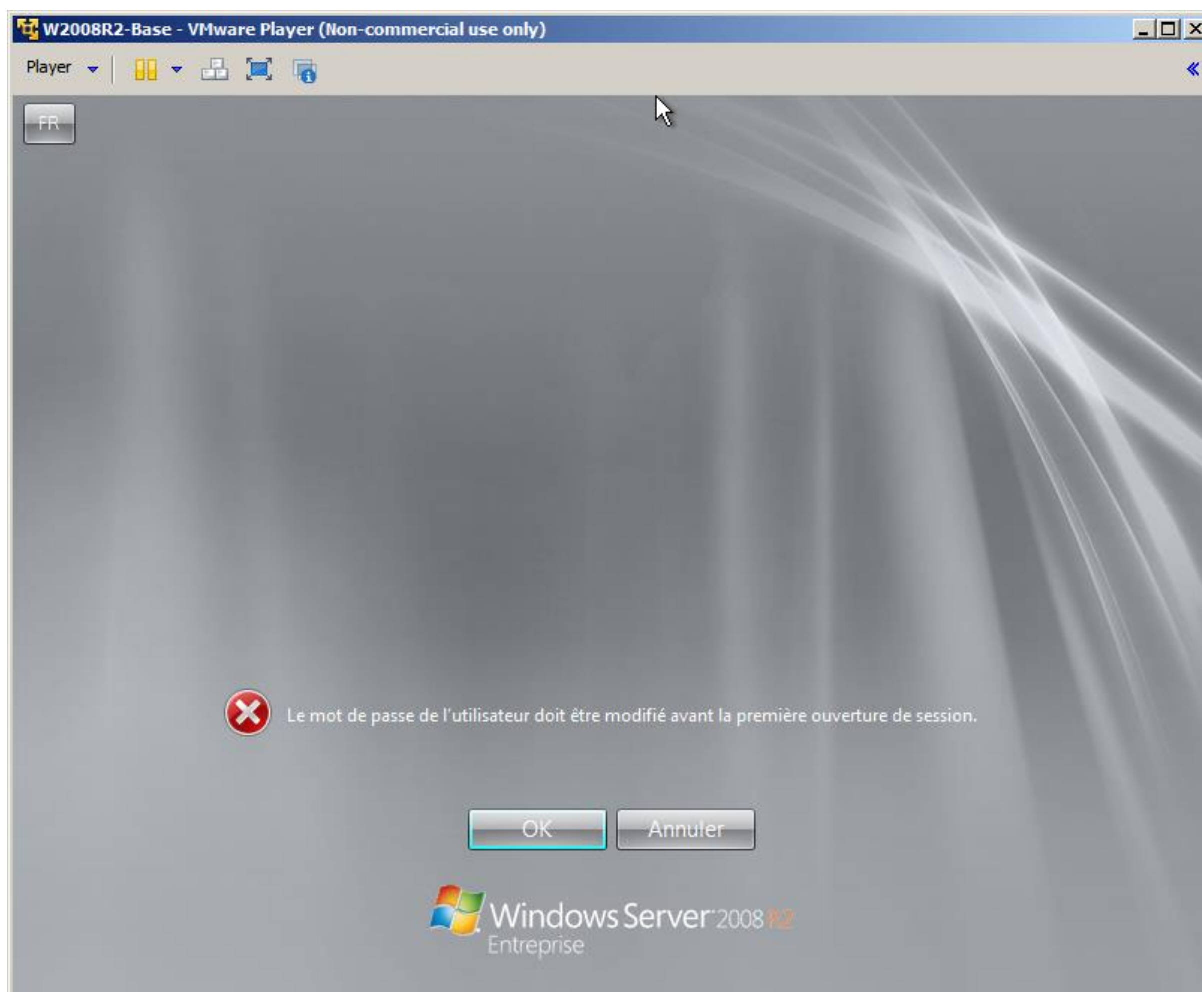


Figure 33 : Windows serveur: Installation: mot de passe administrateur

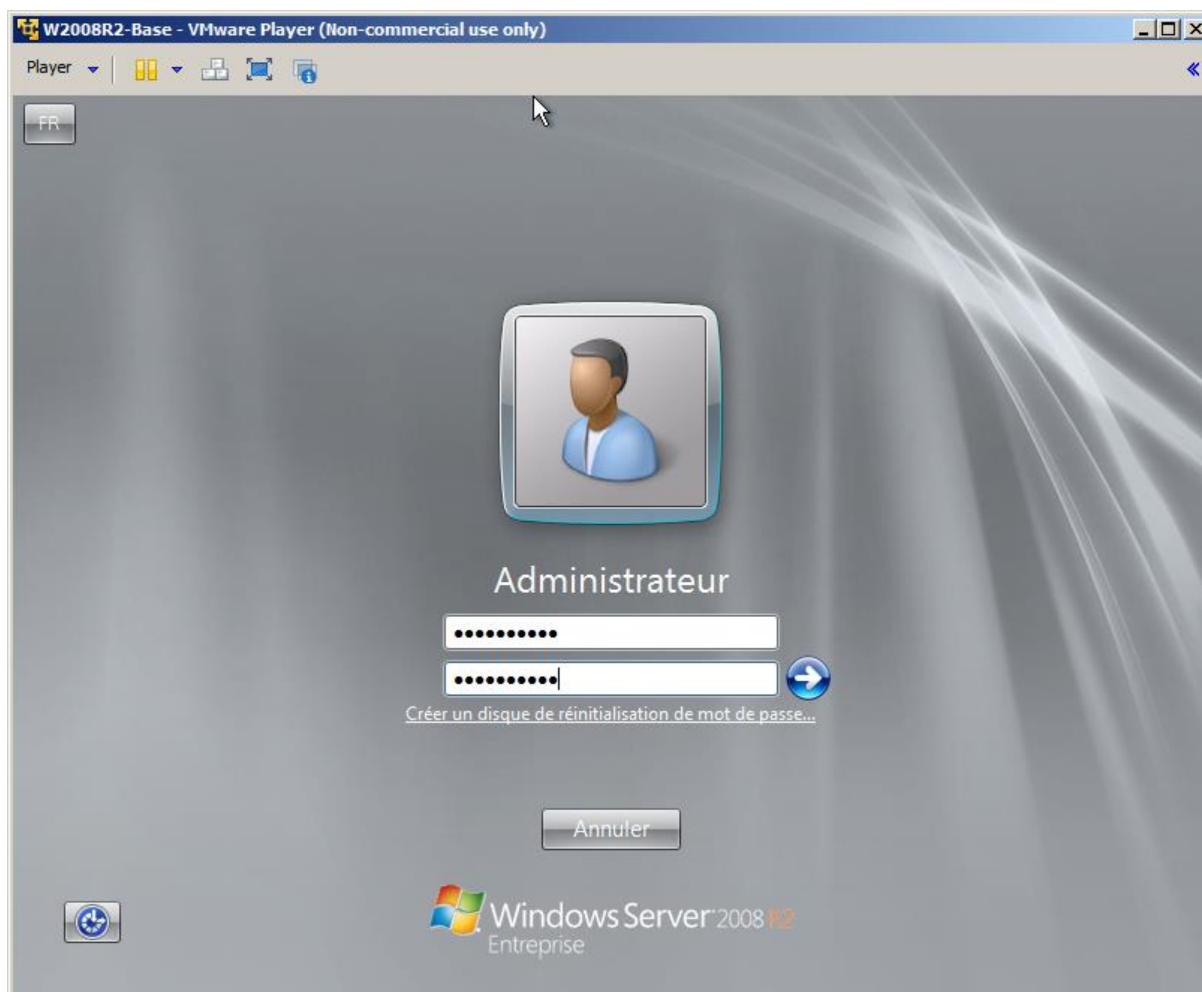


Figure 34 : Windows serveur: Installation: saisie mot de passe administrateur

Conseil : Attention au numlock

Conseil : noter le mot de passe dans le dossier d'exploitation

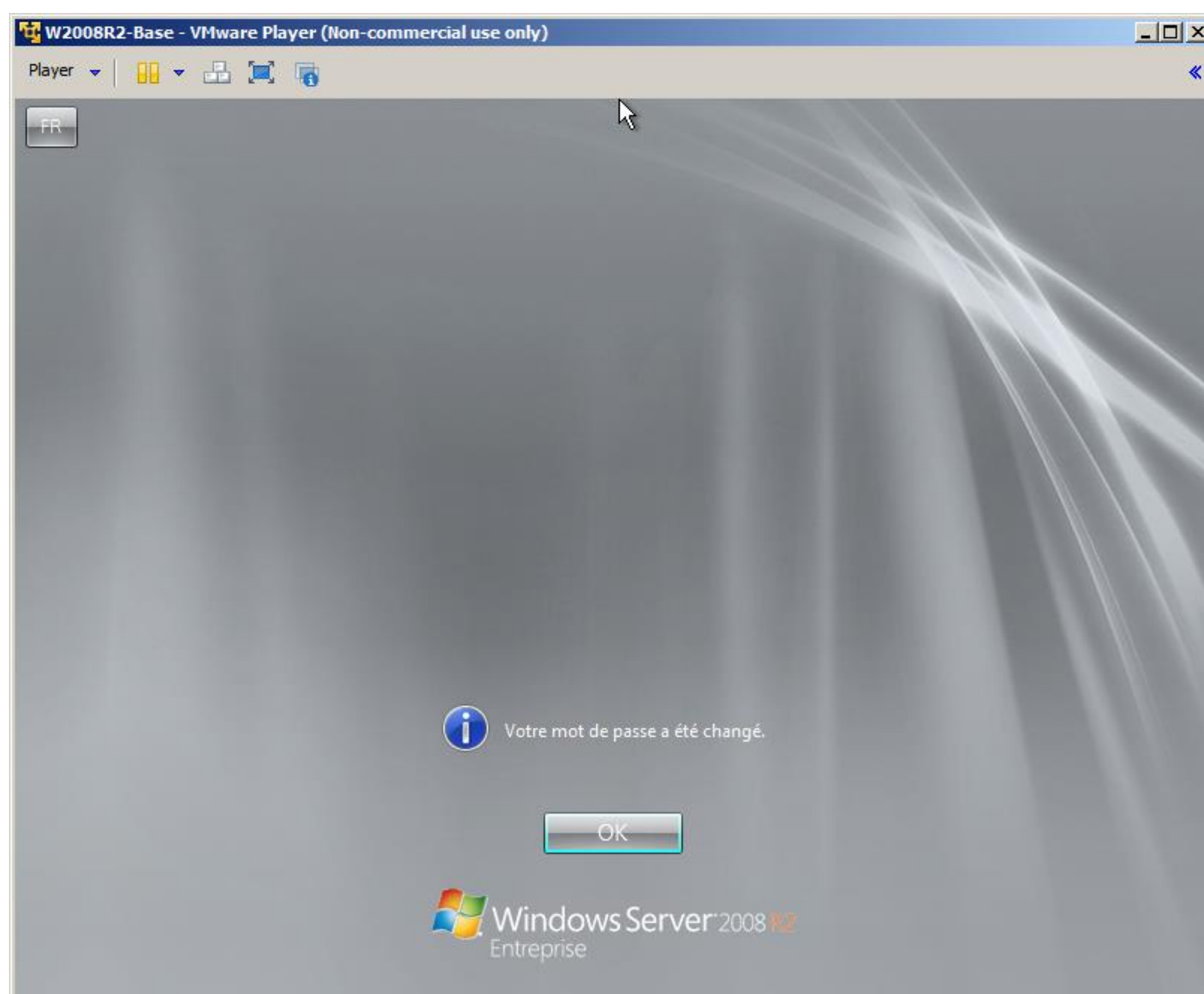


Figure 35 : Windows serveur: Installation: mot de passe administrateur changé

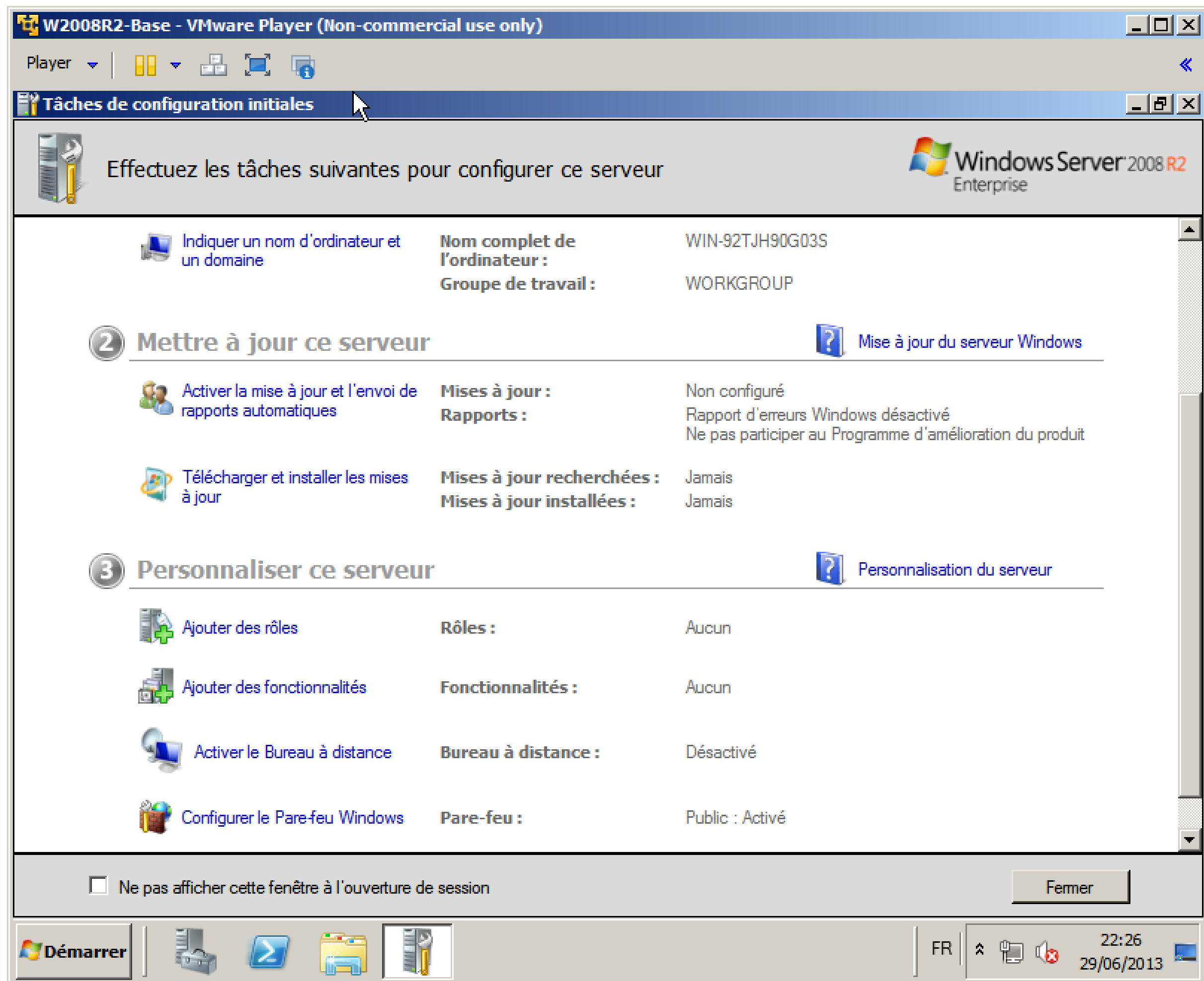


Figure 36 : Windows serveur: Installation: accueil

Conseil: « Démarrer > panneau de configuration > Petites icônes »

Conseil: « Démarrer > panneau de configuration > Options des dossiers > décocher les options « masquer… » »

Conseil: Pour les tests / la configuration du serveur avant la production, désactiver la sécurité renforcée

« **Démarrer > panneau de configuration > Programmes et fonctionnalités > Activer ou désactiver des fonctionnalités de Windows** »

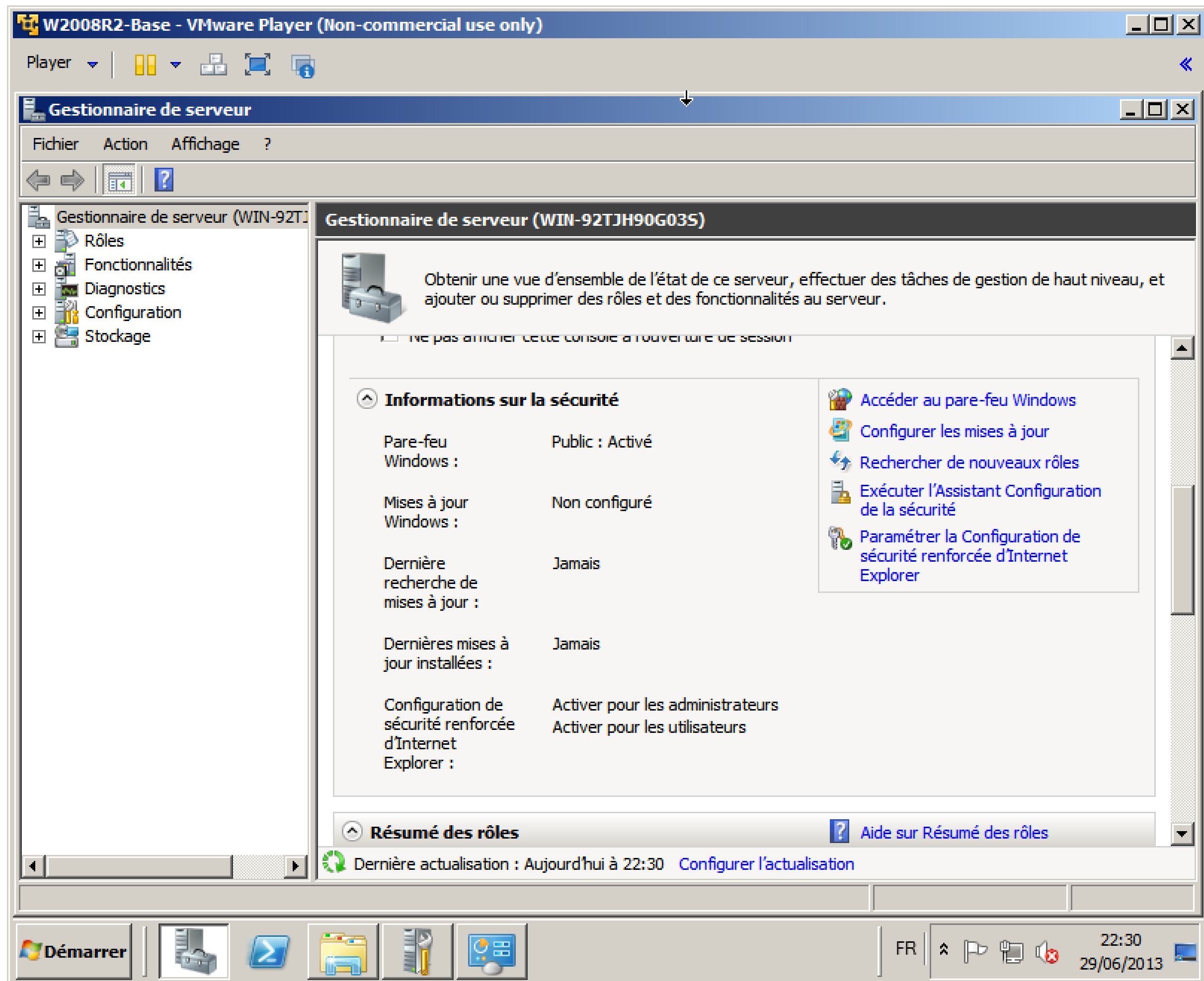


Figure 37 : Windows serveur: Installation: sécurité renforcée

« **Paramétrer la Configuration de sécurité renforcée d'Internet Explorer** > désactivé »

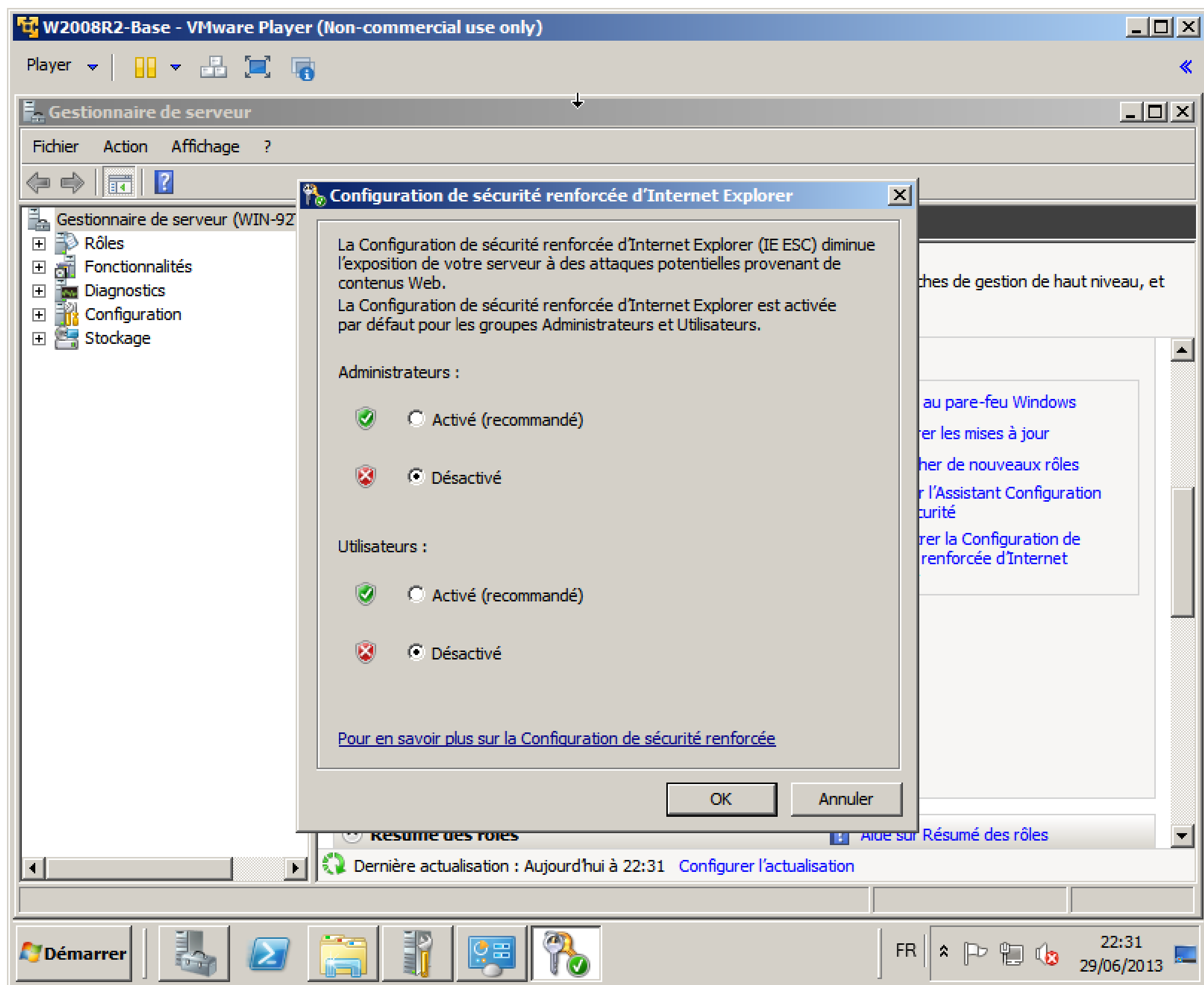


Figure 38 : Windows serveur: Installation: Paramétrage de la sécurité renforcée

Conseil: **Pour la production, réactiver la sécurité renforcée**

Conseil : Pour la production : **désactiver** les mises à jour Windows Update automatique et/ou **utiliser WSUS** (Windows Server Update Services).

Les environnements serveur doivent être des environnements qualifiés, dont la configuration est maitrisée et les changements de configuration décidés et validés.

Les mises à jour doivent être **préalablement effectuées et validées sur des environnements de recette**.

Une fois validées, elles peuvent être propagées sur les environnements de production suivant une procédure clairement définie qui permet d'anticiper les impacts pour les utilisateurs et sur les applications.

Ces bonnes pratiques concernent aussi bien Windows que les applications tierces.

Ceci concerne en particulier Java, dont les mises à jour automatiques doivent être impérativement désactivées sur les serveurs, **une veille des mises à jour Java doit être mise en place et les mises à jour doivent être préalablement recettées avant mise en production.**

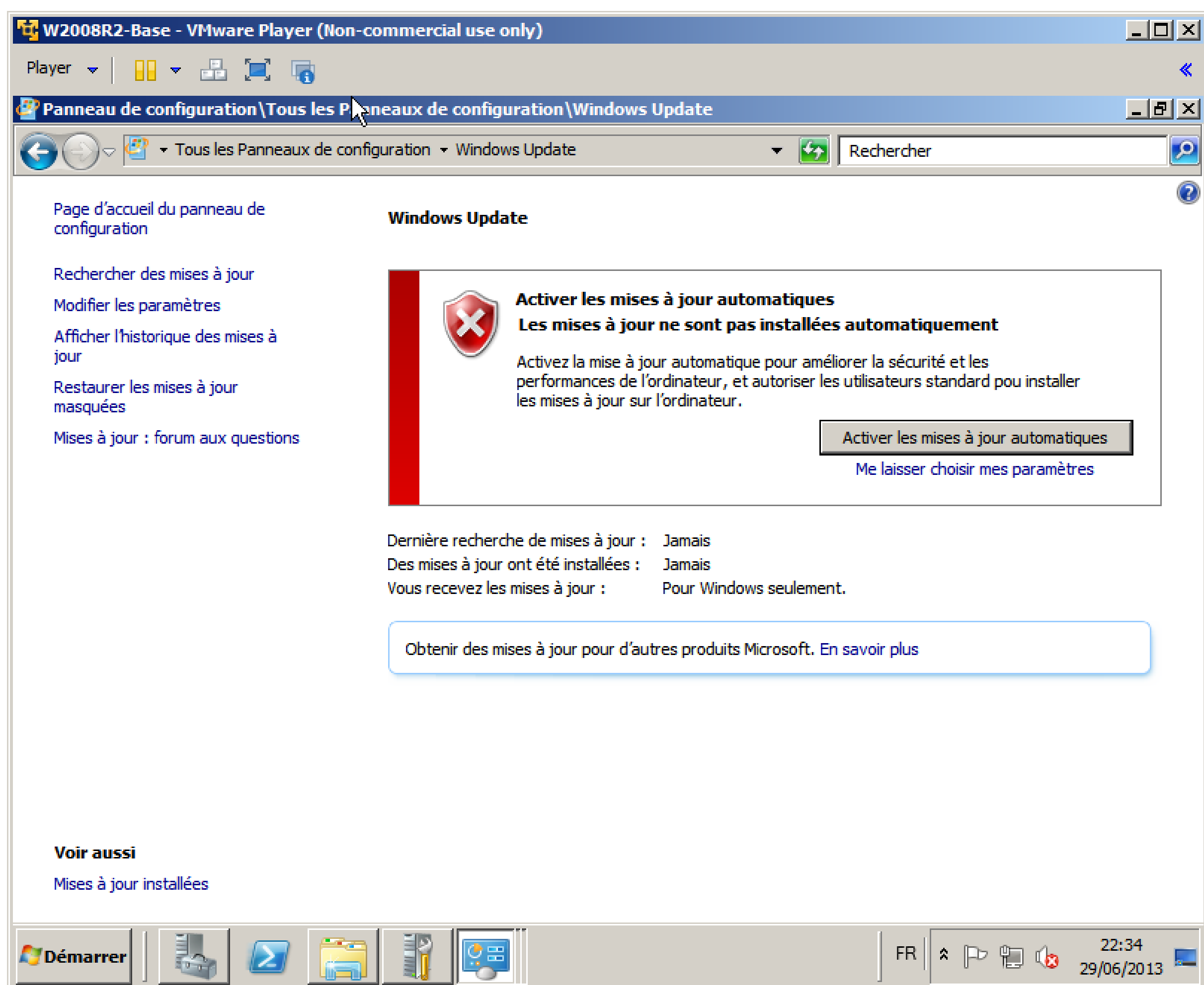


Figure 39 : Windows serveur: Configuration: maitriser les mises à jour

« Modifier les paramètres »

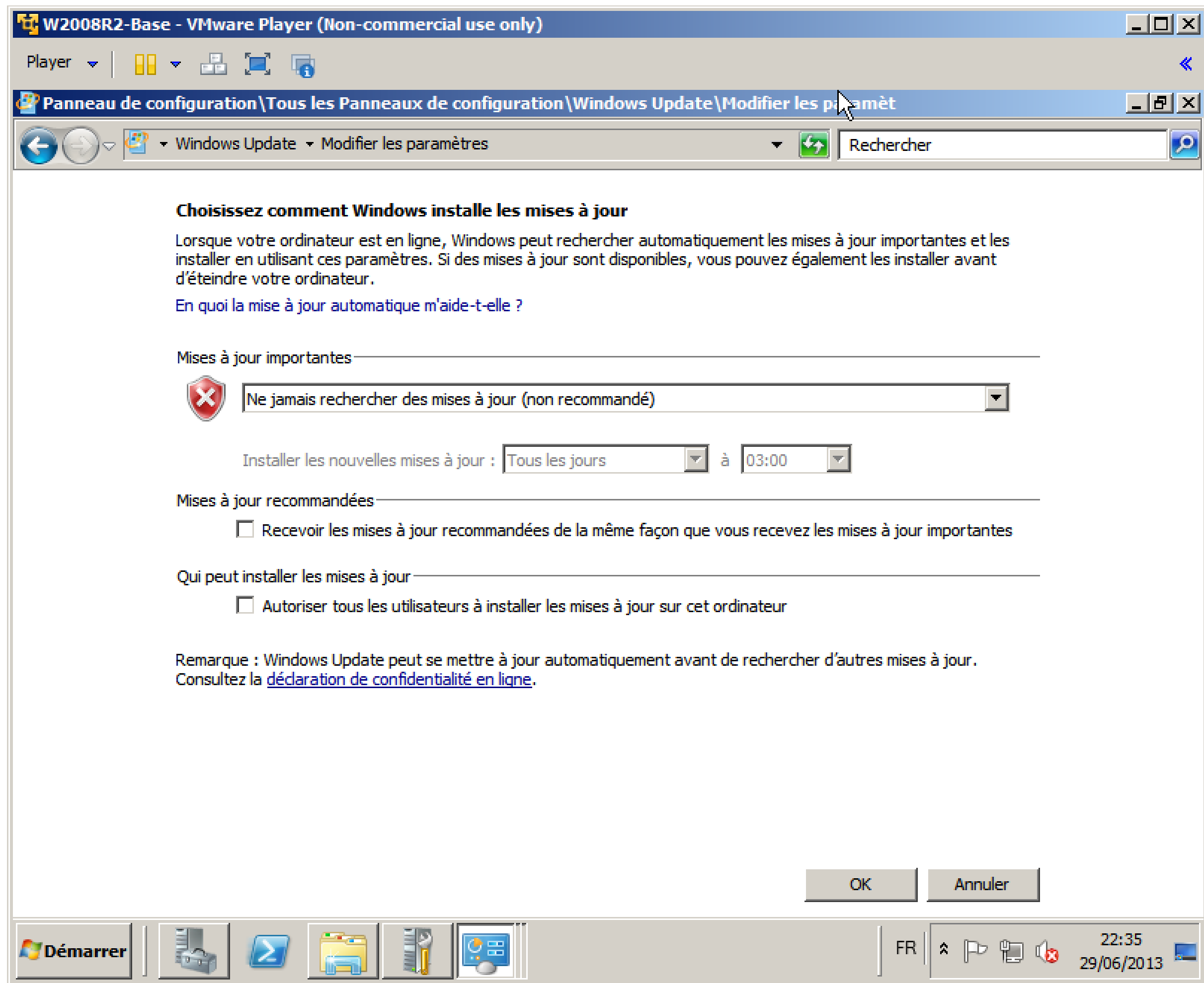


Figure 40 : Windows serveur: Configuration: maitriser les mises à jour

Conseil : A ce stade : changer le nom de la machine : **Start**, click **Run…**, **cmd**, **control system, Paramètres système avancés, nom de l'ordinateur.**

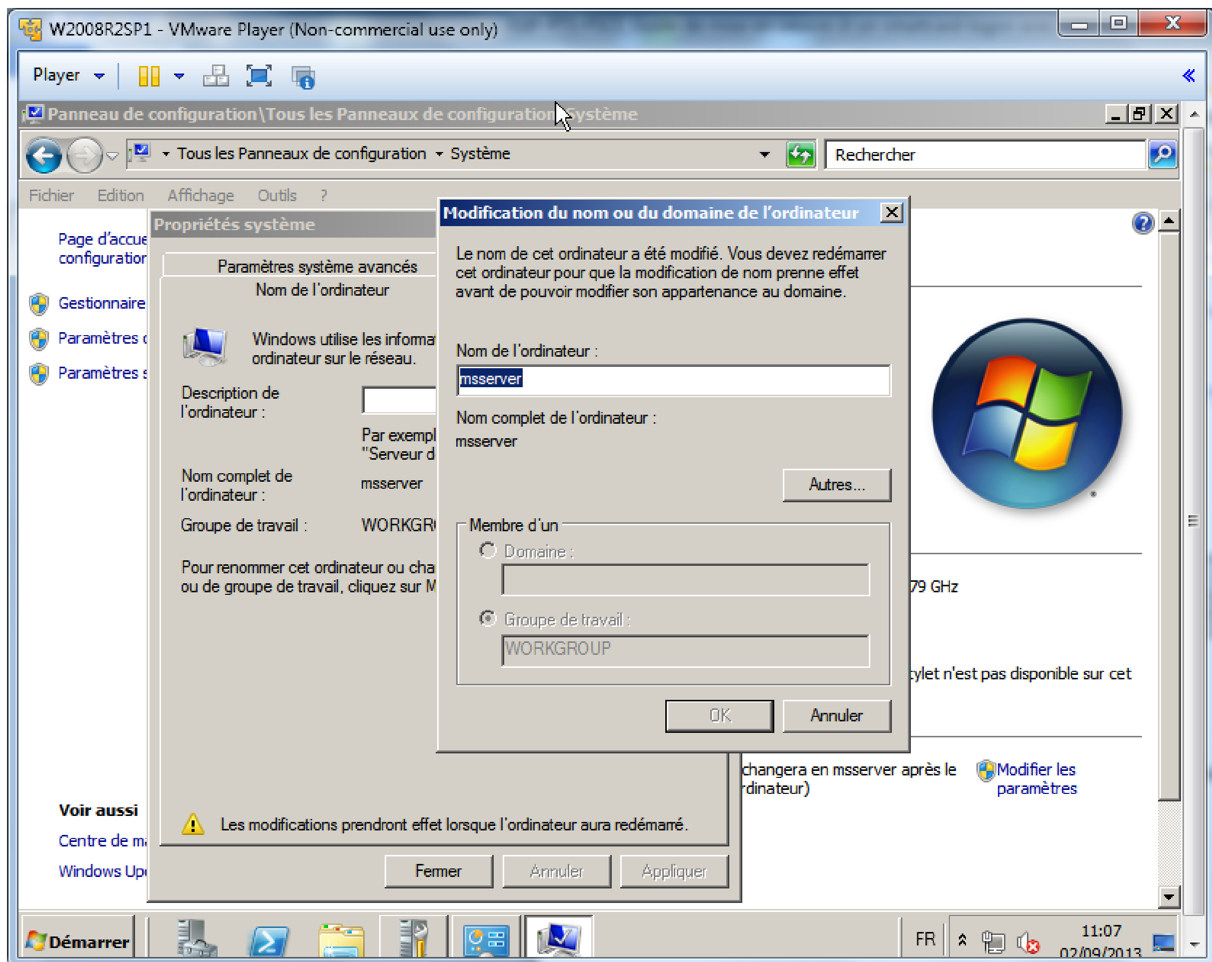


Figure 41 : Windows serveur: Configuration: nom de l'ordinateur

12.4 Installation d'un rôle Active Directory

Le rôle Active Directory s'installe en ajoutant le rôle « **Services de domaine Active Directory** » :

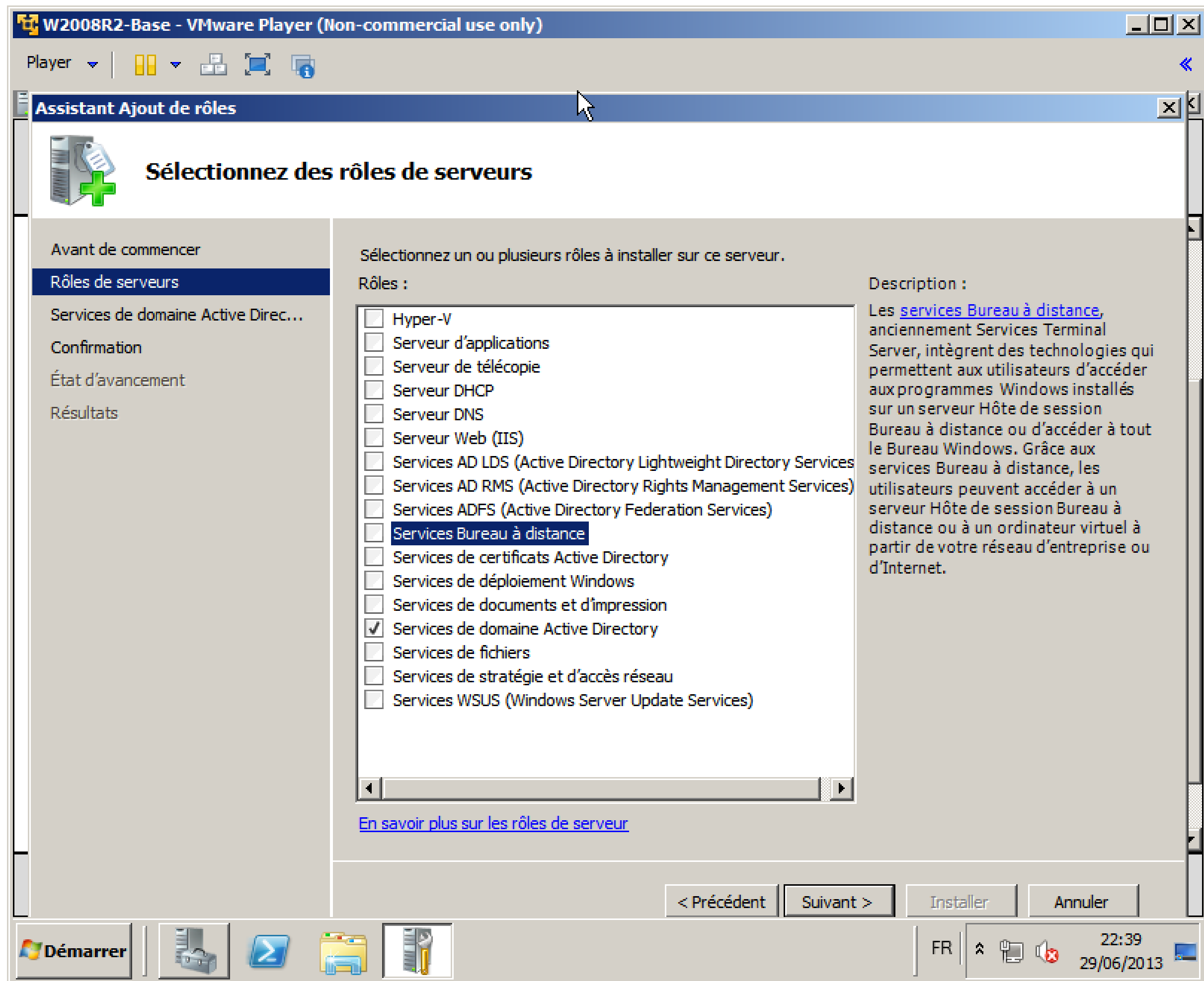


Figure 42 : Active Directory: Installation du rôle

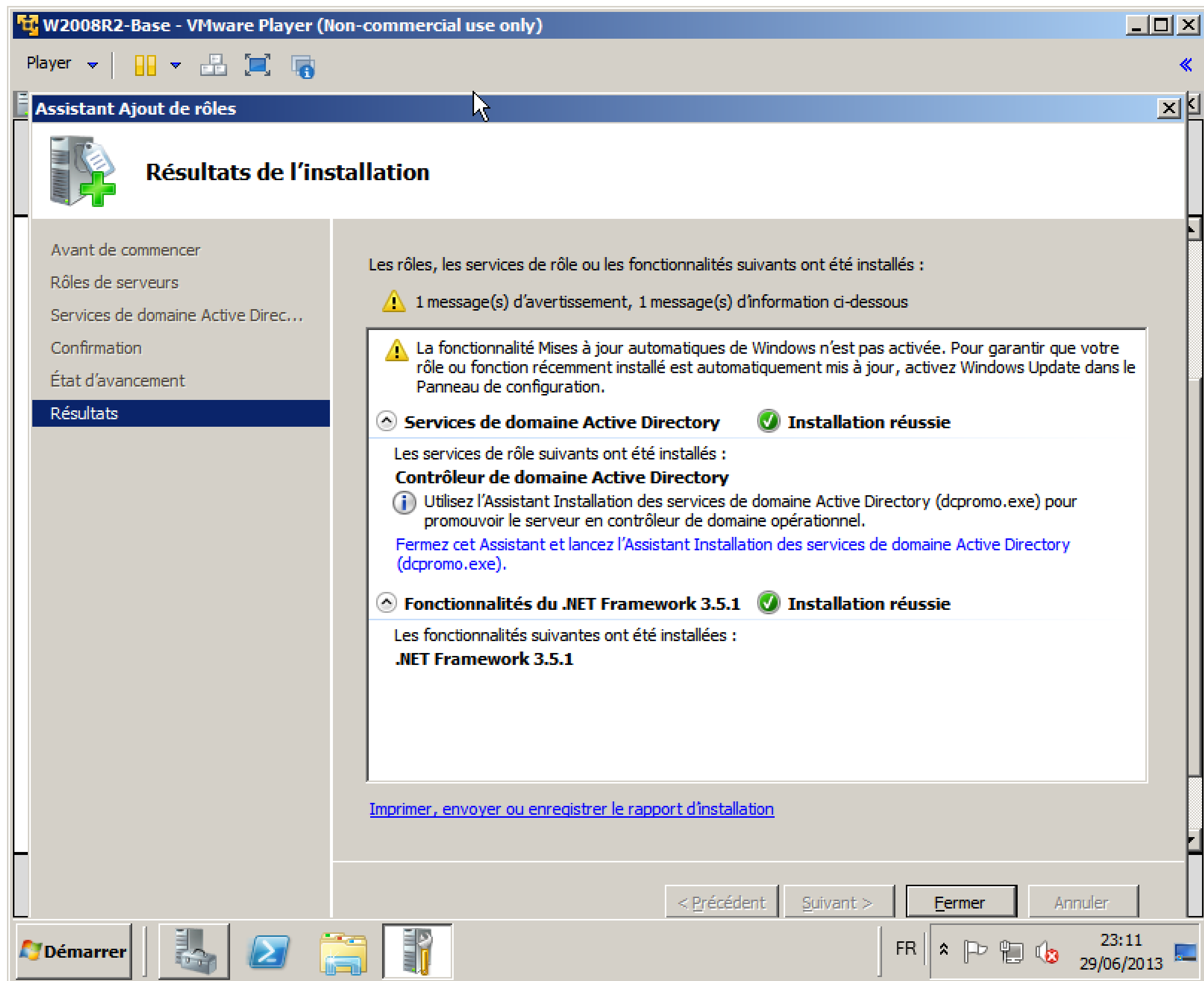


Figure 43 : Active Directory: Installation du rôle : résultat

Promouvoir le serveur en tant que contrôleur de domaine Active Directory en lancant l'assistant « **dcpromo.exe** » (le serveur devra rebooter à la fin de cette phase) :

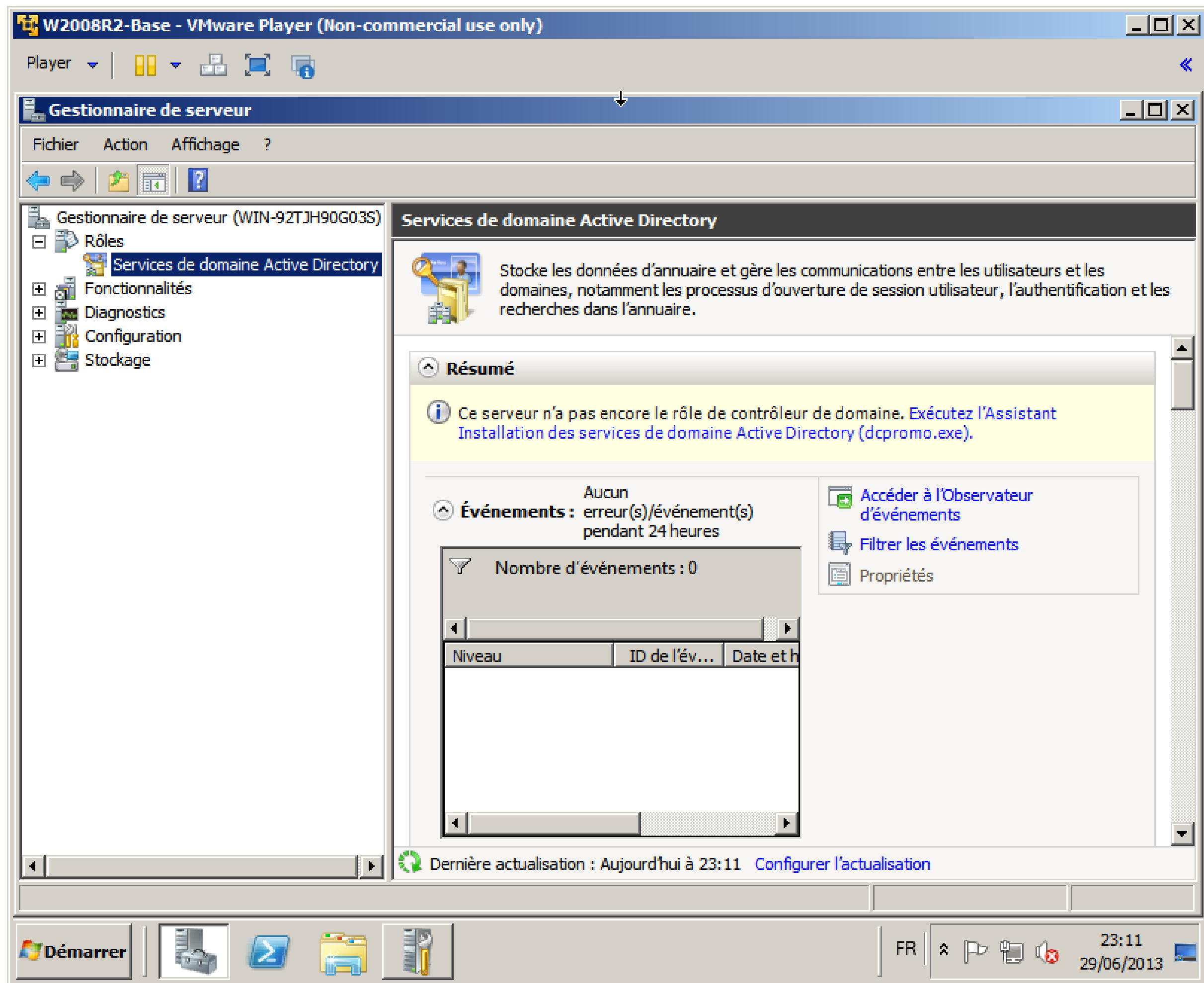


Figure 44 : Active Directory: Configuration du rôle

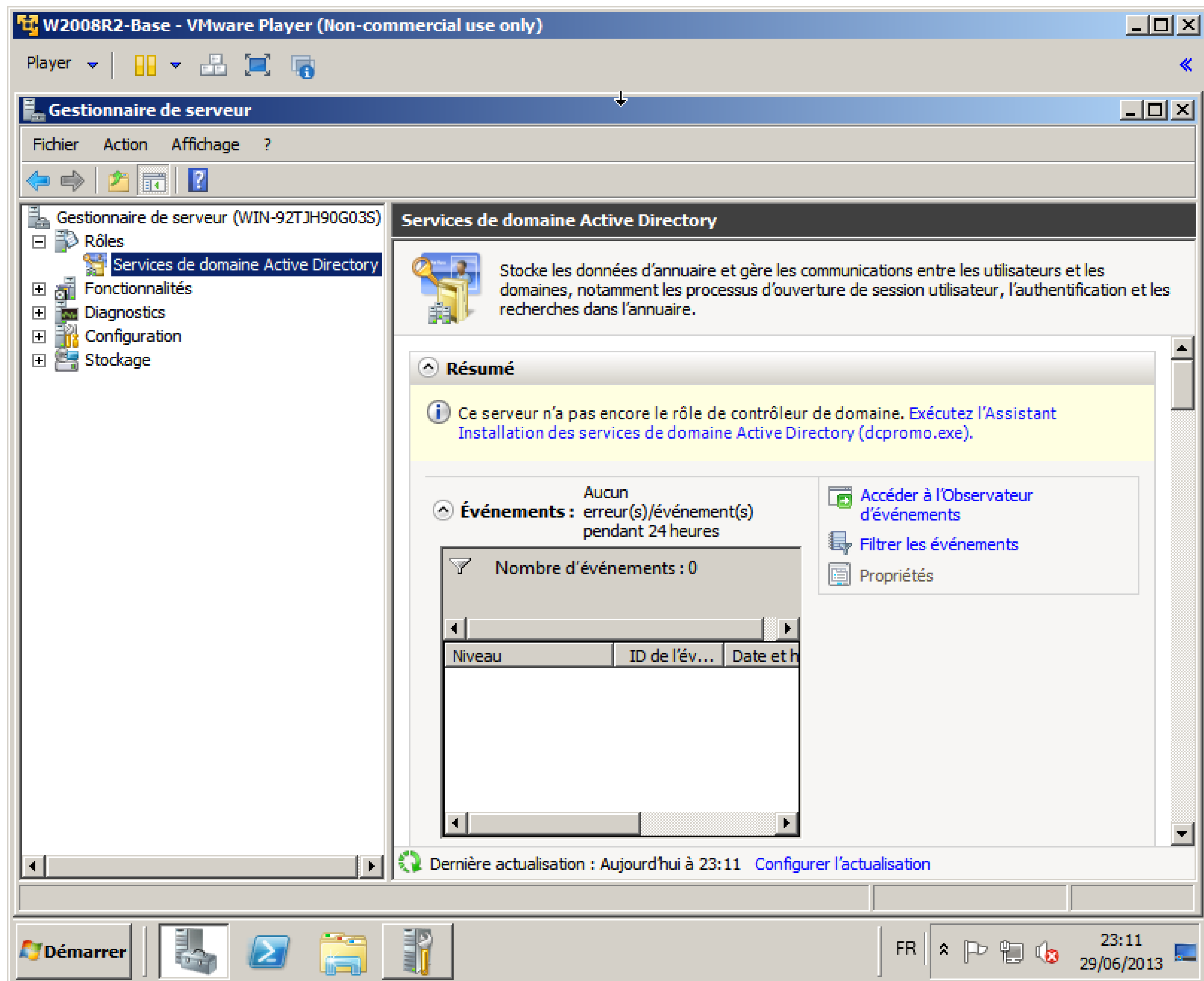


Figure 45 : Active Directory: Configuration du rôle : Exécution de l'assistant

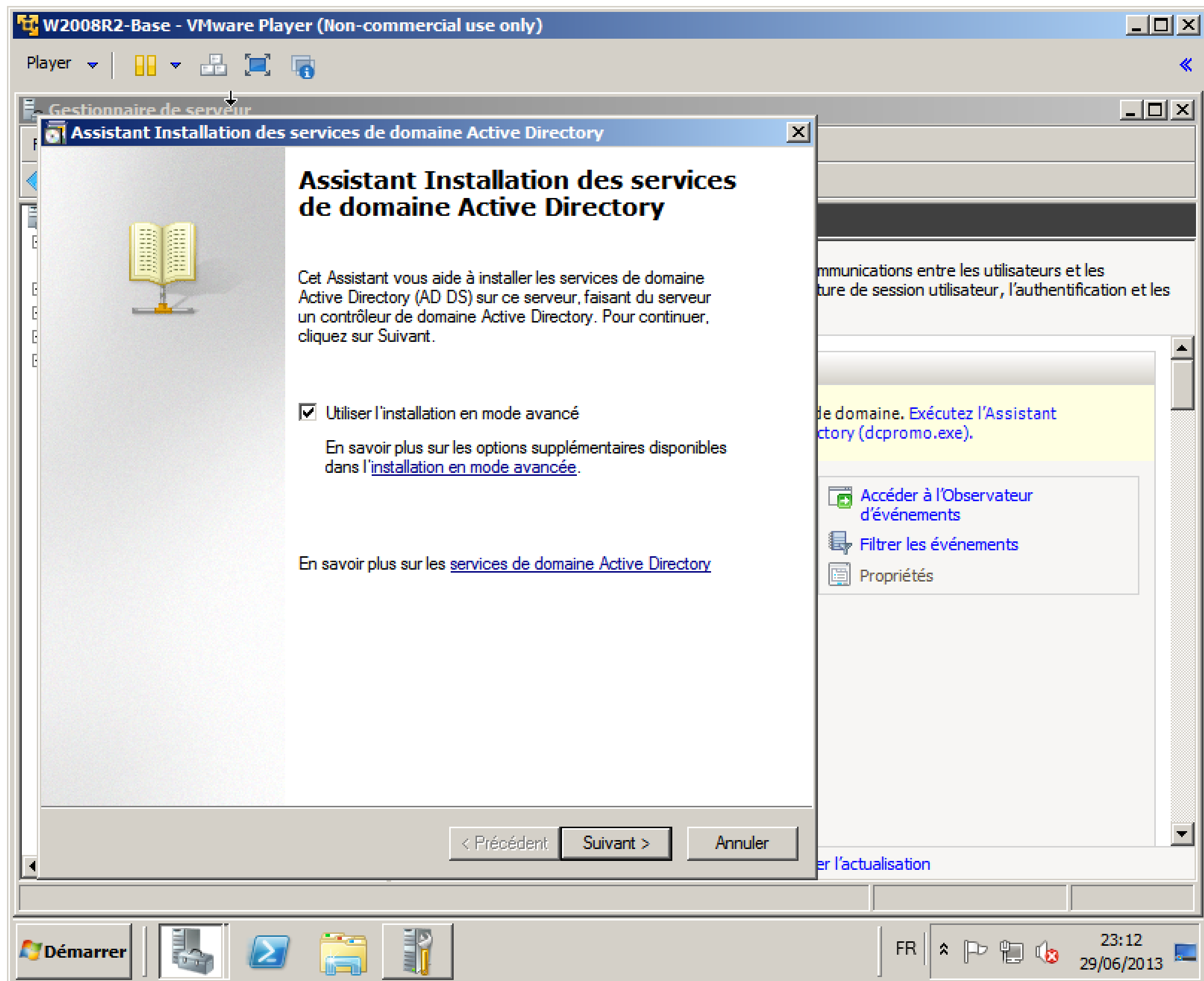


Figure 46 : Active Directory: Configuration du rôle : mode avancé

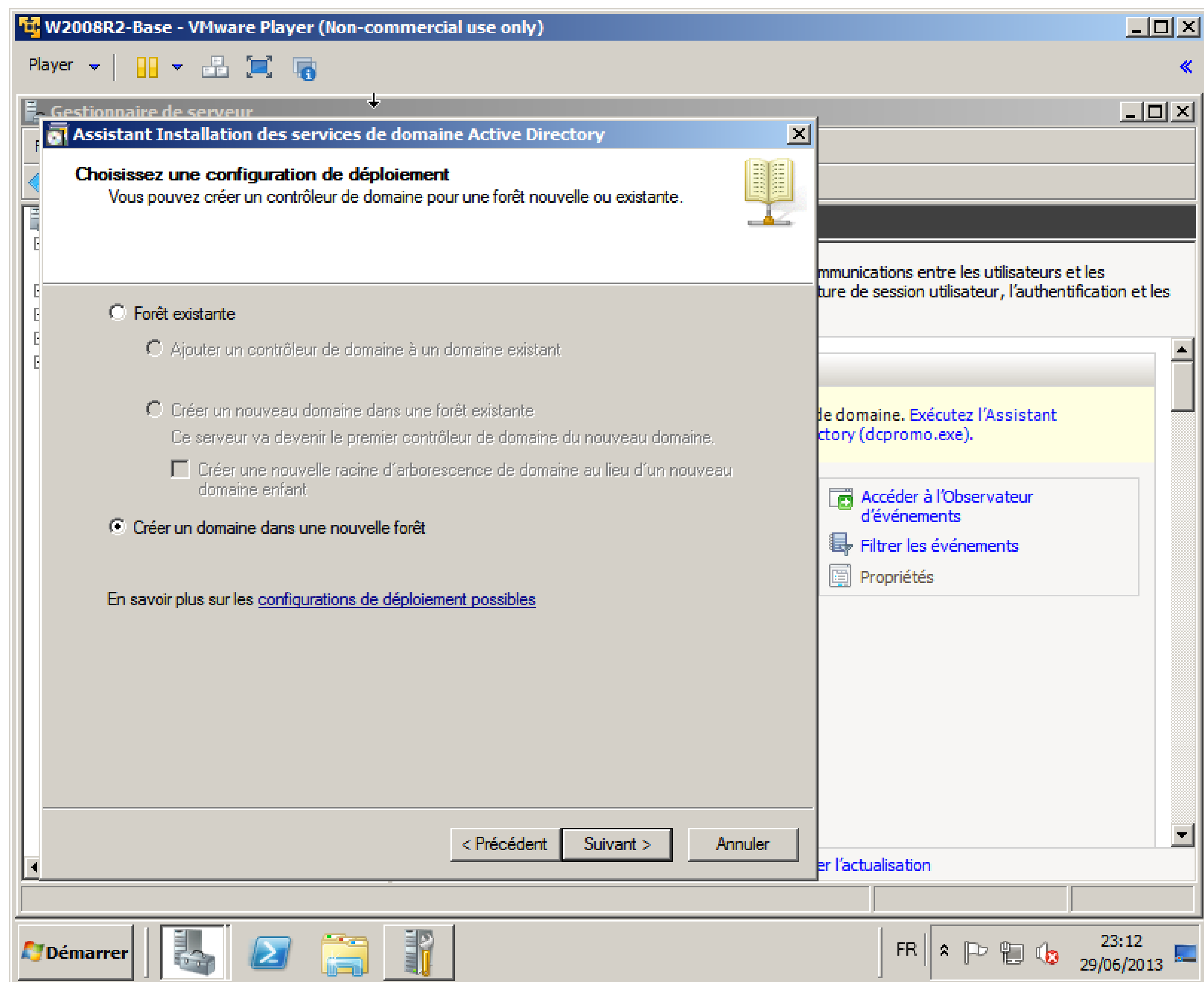


Figure 47 : Active Directory: Configuration du rôle : nouvelle forêt

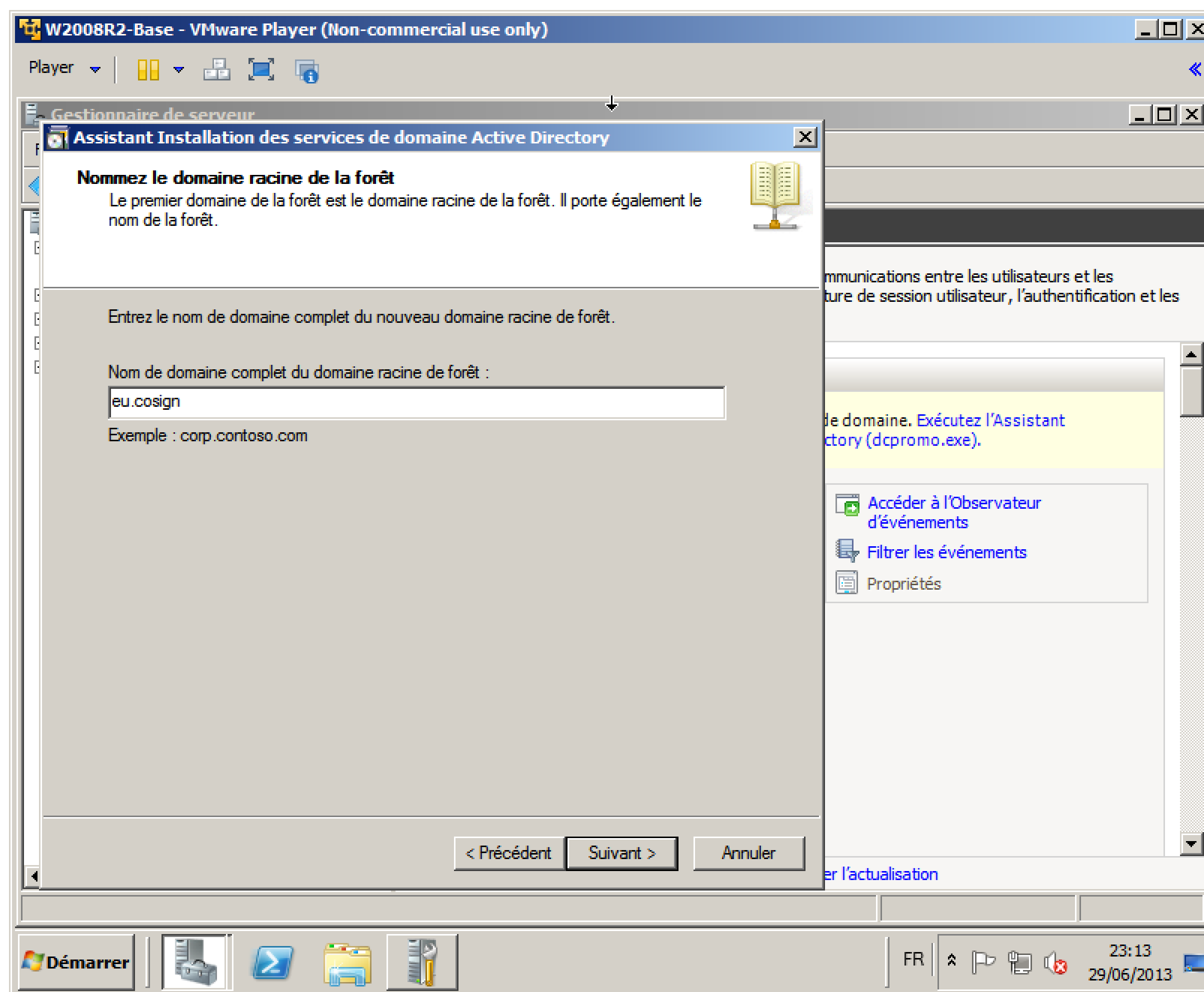


Figure 48 : Active Directory: Configuration du rôle : nom de domaine

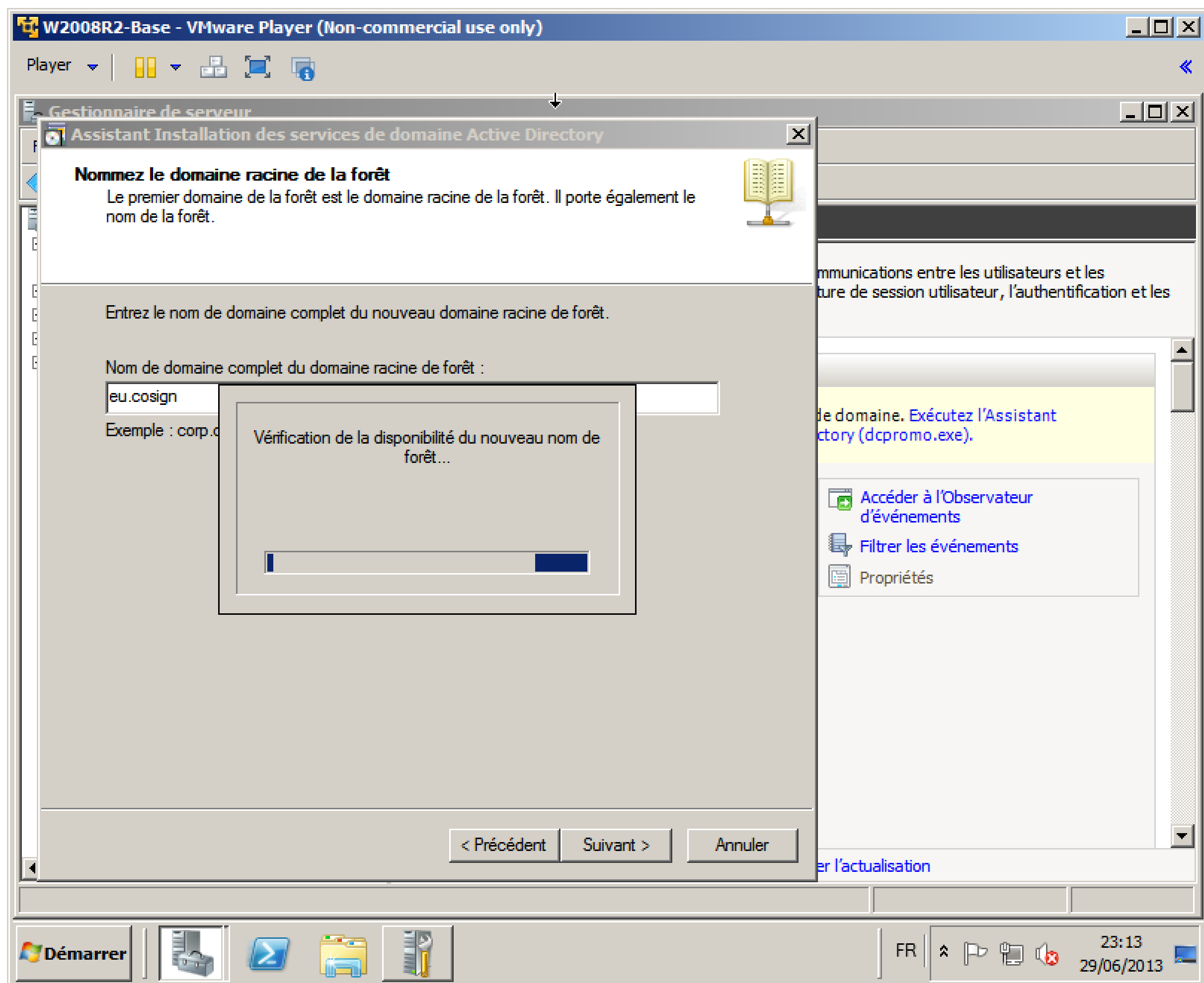


Figure 49 : Active Directory: Configuration du rôle : vérification de la disponibilité du nom de la forêt

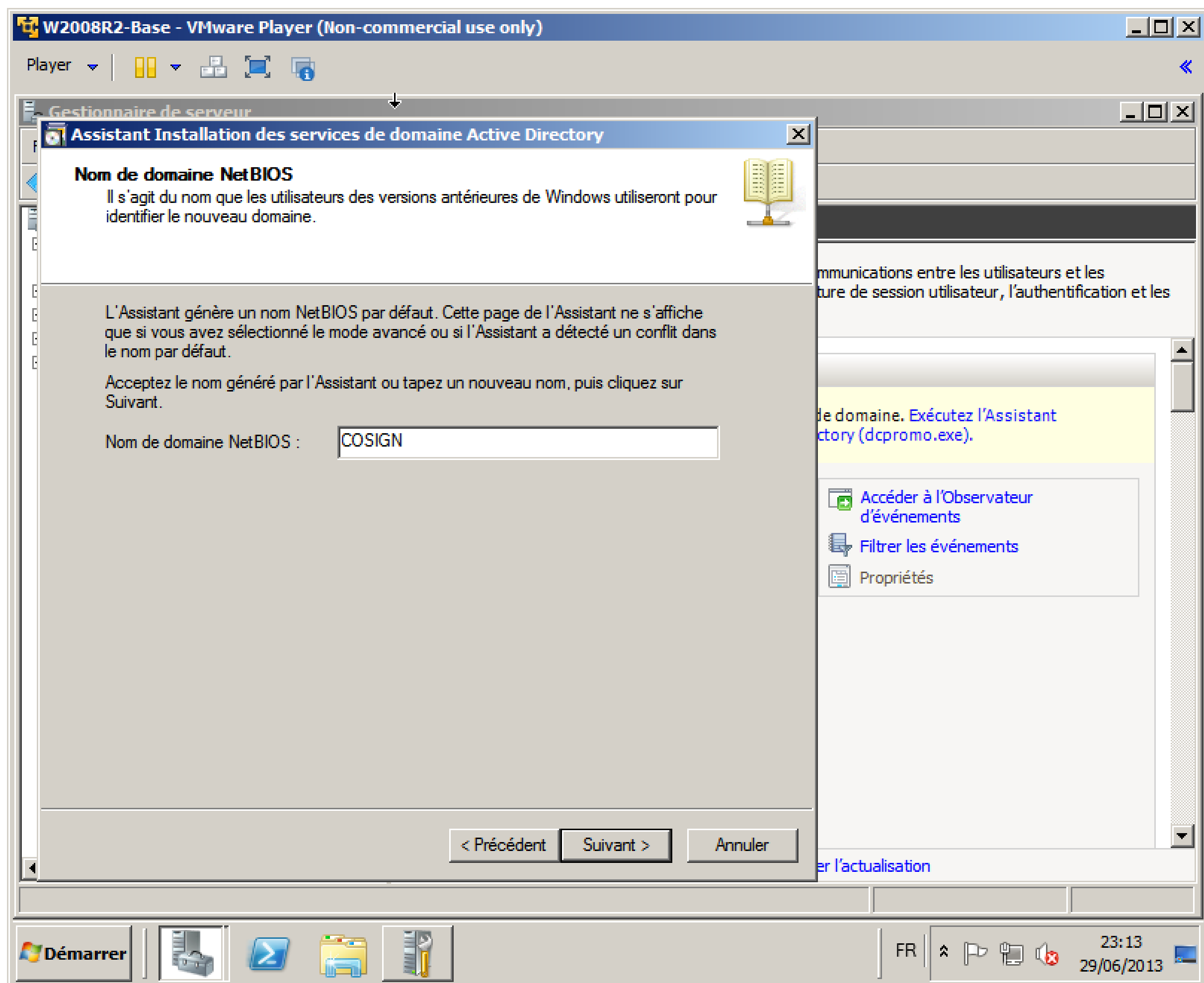


Figure 50 : Active Directory: Configuration du rôle : NetBIOS

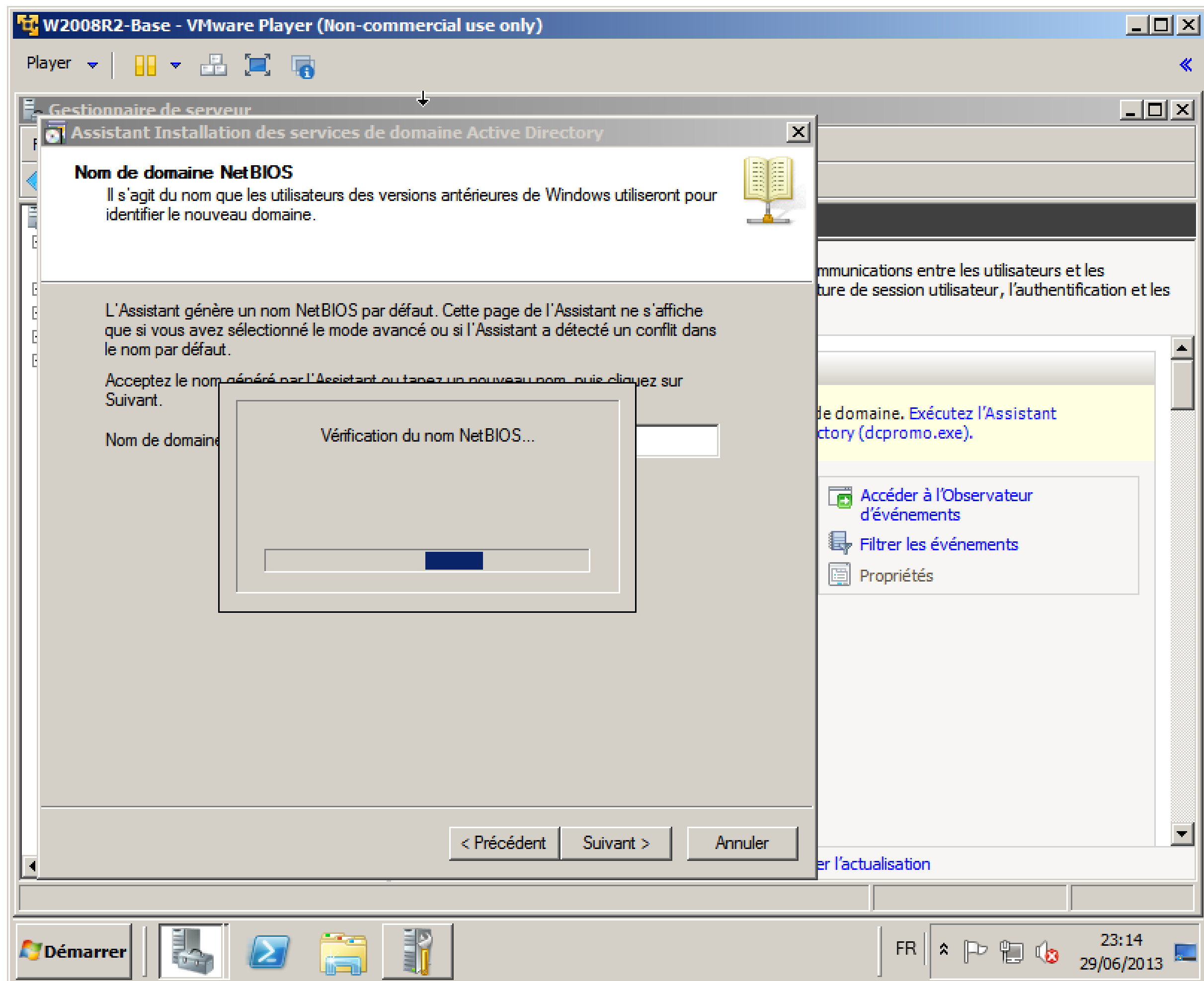


Figure 51 : Active Directory: Configuration du rôle : Vérif. NetBIOS

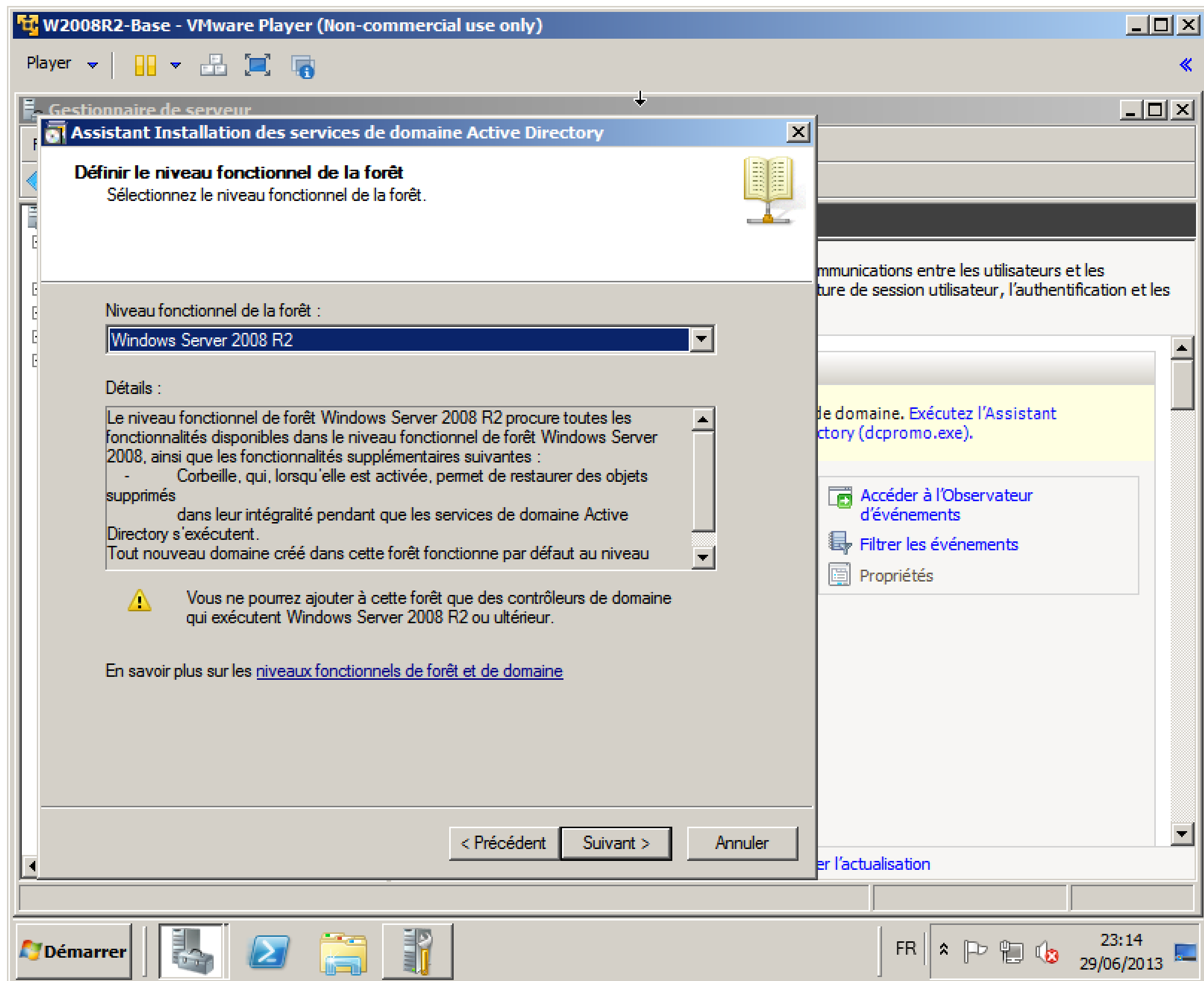


Figure 52 : Active Directory: Configuration du rôle : Niveau fonctionnel

L'étape suivante « Analyse de la configuration DNS » peut prendre du temps :

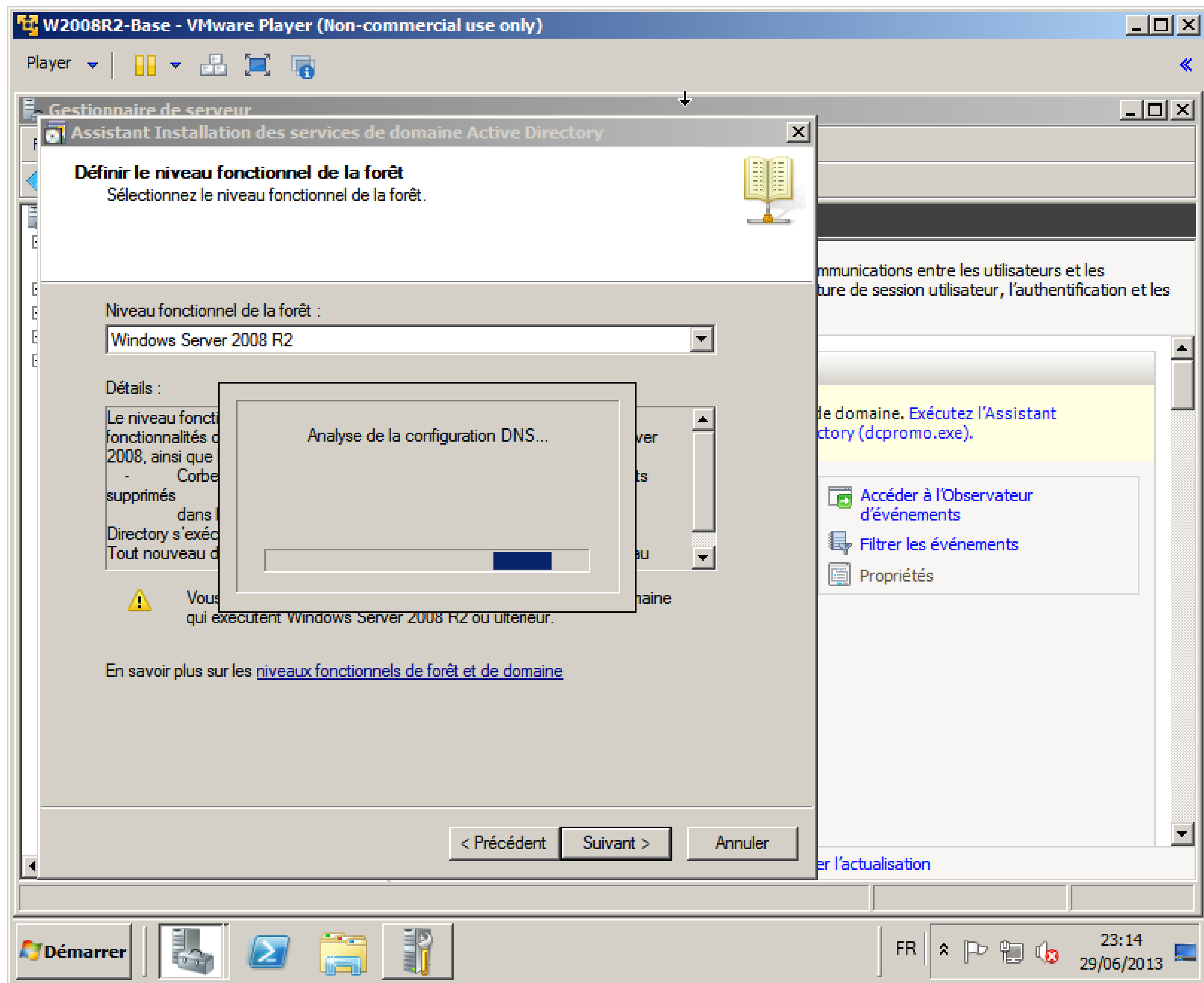


Figure 53 : Active Directory: Configuration du rôle : Configuration DNS

A priori, **décocher** l'option « **Serveur DNS** ». A défaut, bien maitriser cette option, sous peine de faire dysfonctionner le réseau sur lequel le serveur est installé.

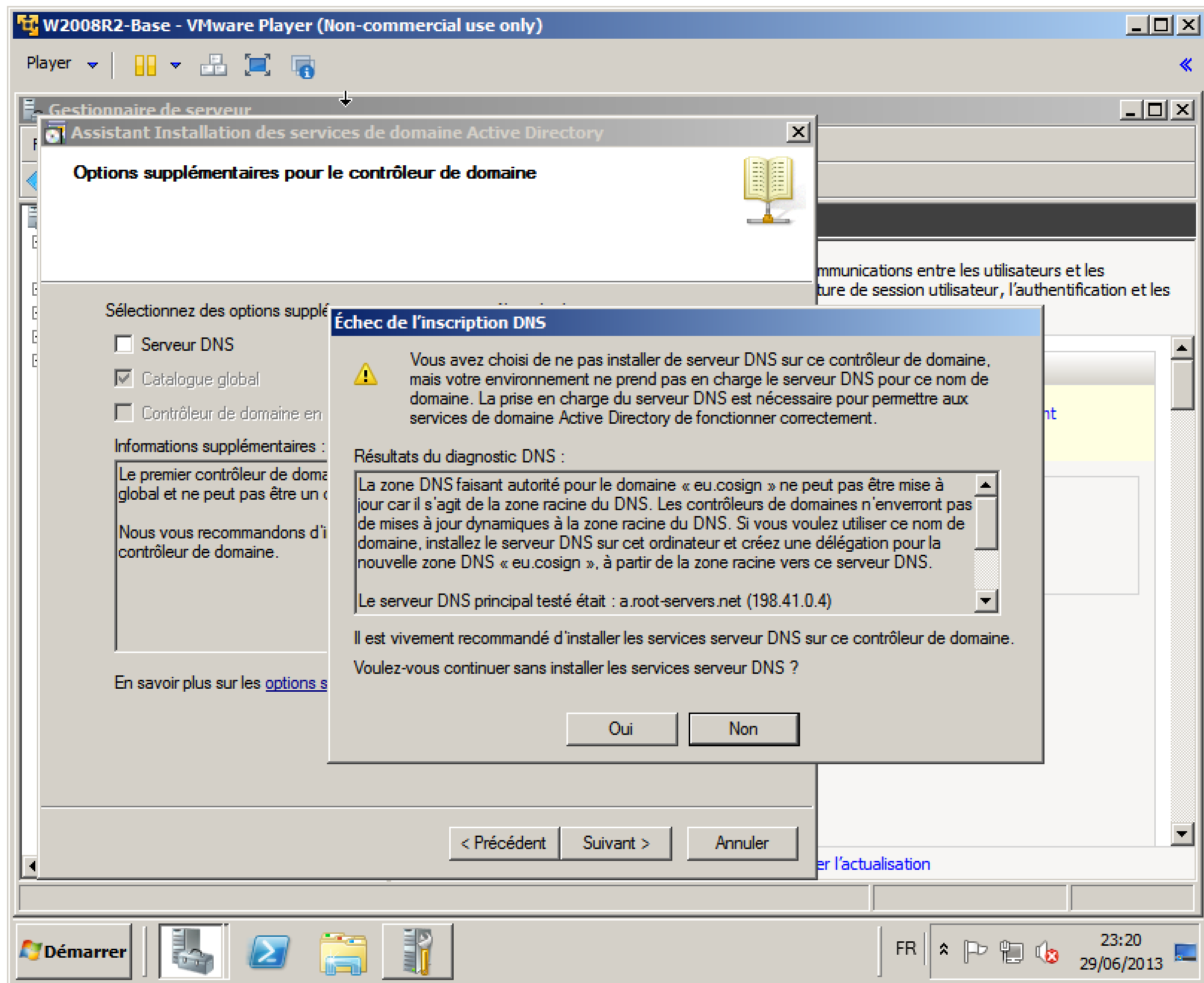


Figure 54 : Active Directory: Configuration du rôle : Décocher DNS

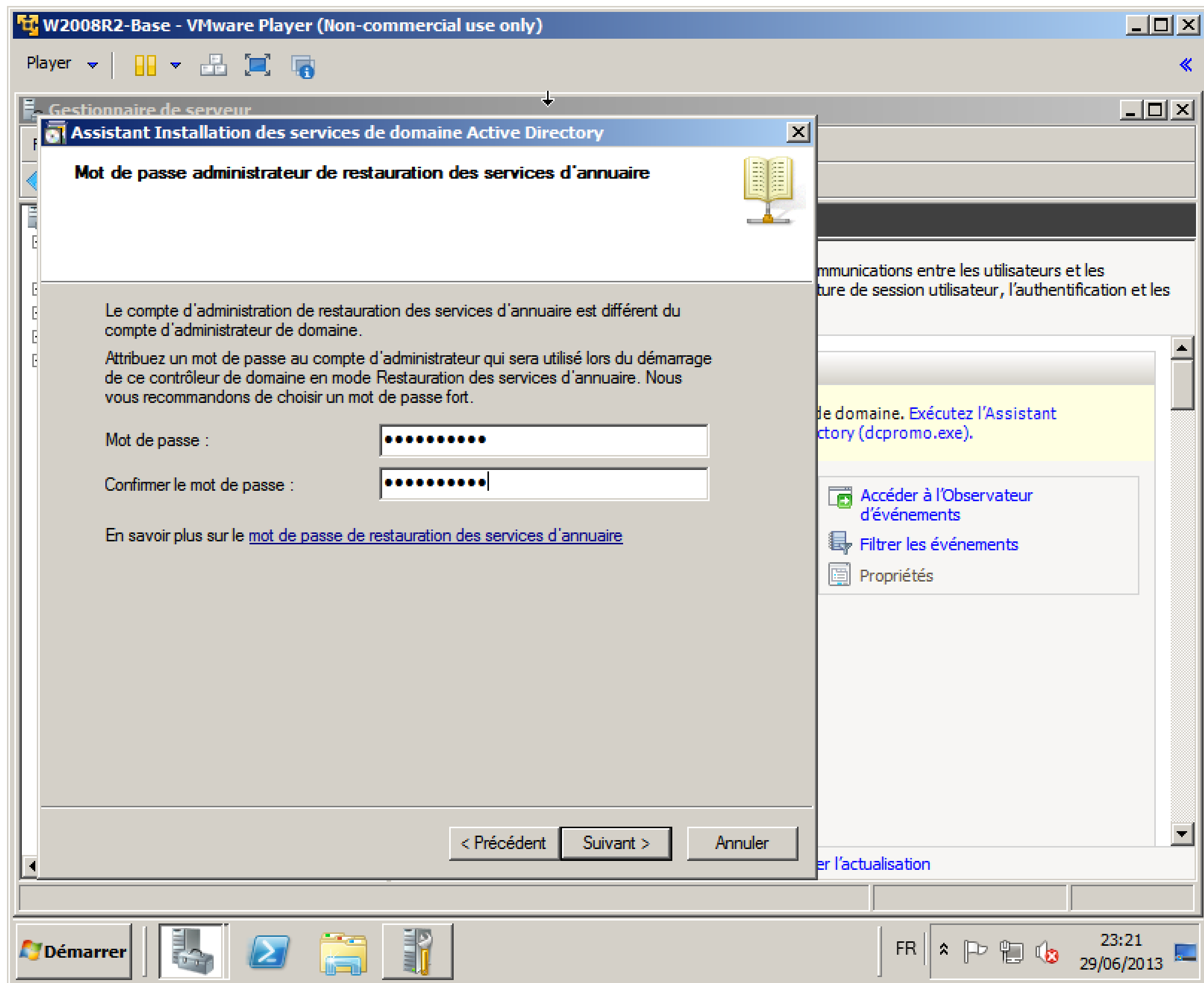


Figure 55 : Active Directory: Configuration du rôle : mot de passe LDAP

Conseil : Noter le mot de passe saisi dans le dossier d'exploitation

Assistant Installation des services de domaine Active Directory

Emplacement de la base de données, des fichiers journaux et de SYSVOL
Spécifiez les dossiers qui contiendront la base de données du contrôleur de domaine Active Directory, les fichiers journaux et SYSVOL.

Pour de meilleures performances et une meilleure récupération, stockez la base de données et les fichiers journaux sur des volumes séparés.

Dossier de la base de données :
C:\Windows\NTDS Parcourir...

Dossier des fichiers journaux :
C:\Windows\NTDS Parcourir...

Dossier SYSVOL :
C:\Windows\SYSVOL Parcourir...

En savoir plus sur le placement des fichiers des services de domaine Active Directory

< Précédent Suivant > Annuler

Figure 56 : Active Directory: Configuration du rôle : configuration des bases de données

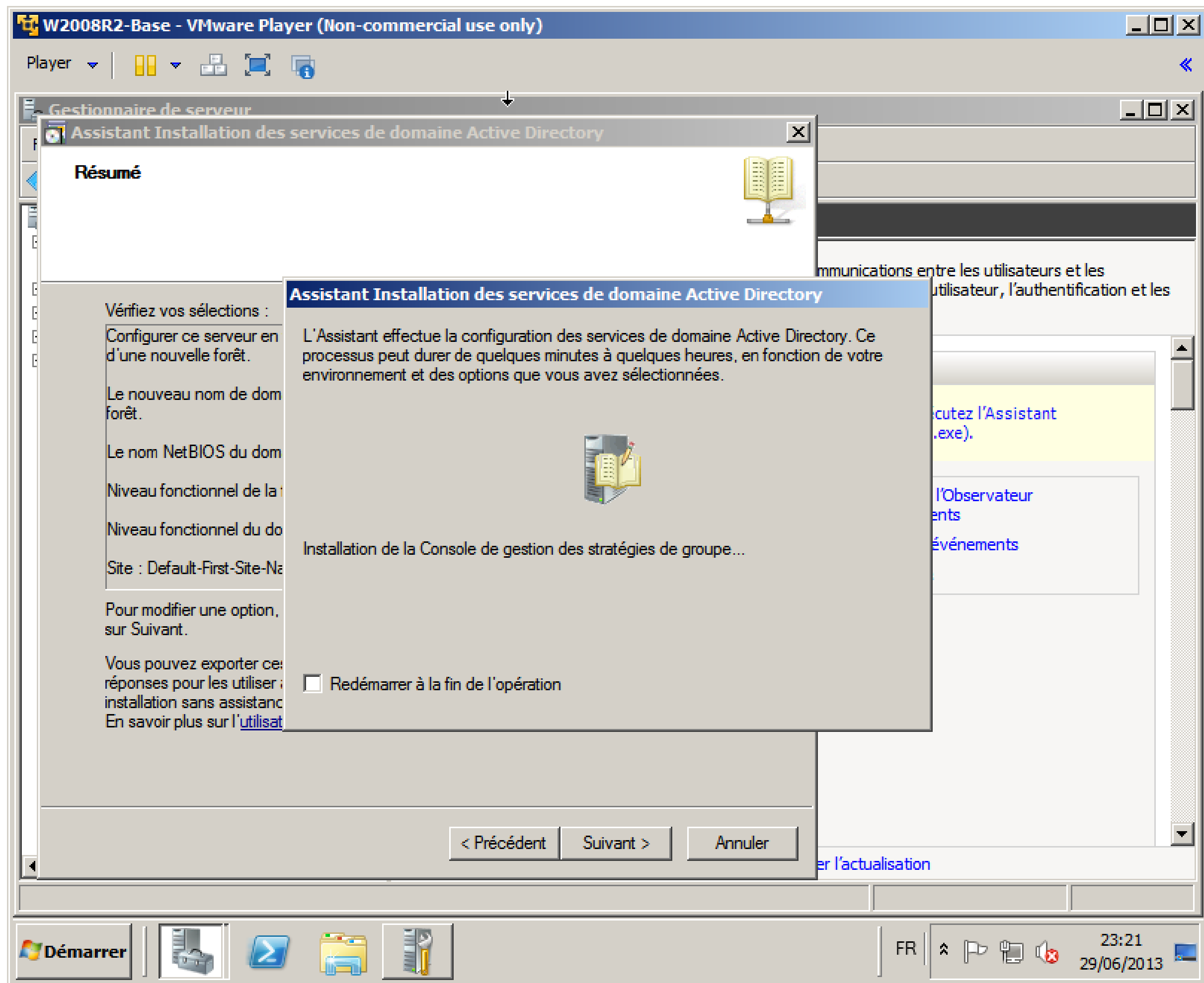


Figure 57 : Active Directory: Configuration du rôle : Installation GPMC

12.5 Installation d'un rôle Certificate Server

Sous **Windows 2008R2**, le rôle Certificate Server s'installe en ajoutant le rôle « **Services de certificats Active Directory** ».

Conseil : bien revérifier les noms de la machine et du domaine car ils ne pourront plus être modifiés une fois le rôle Certificate Server installé.

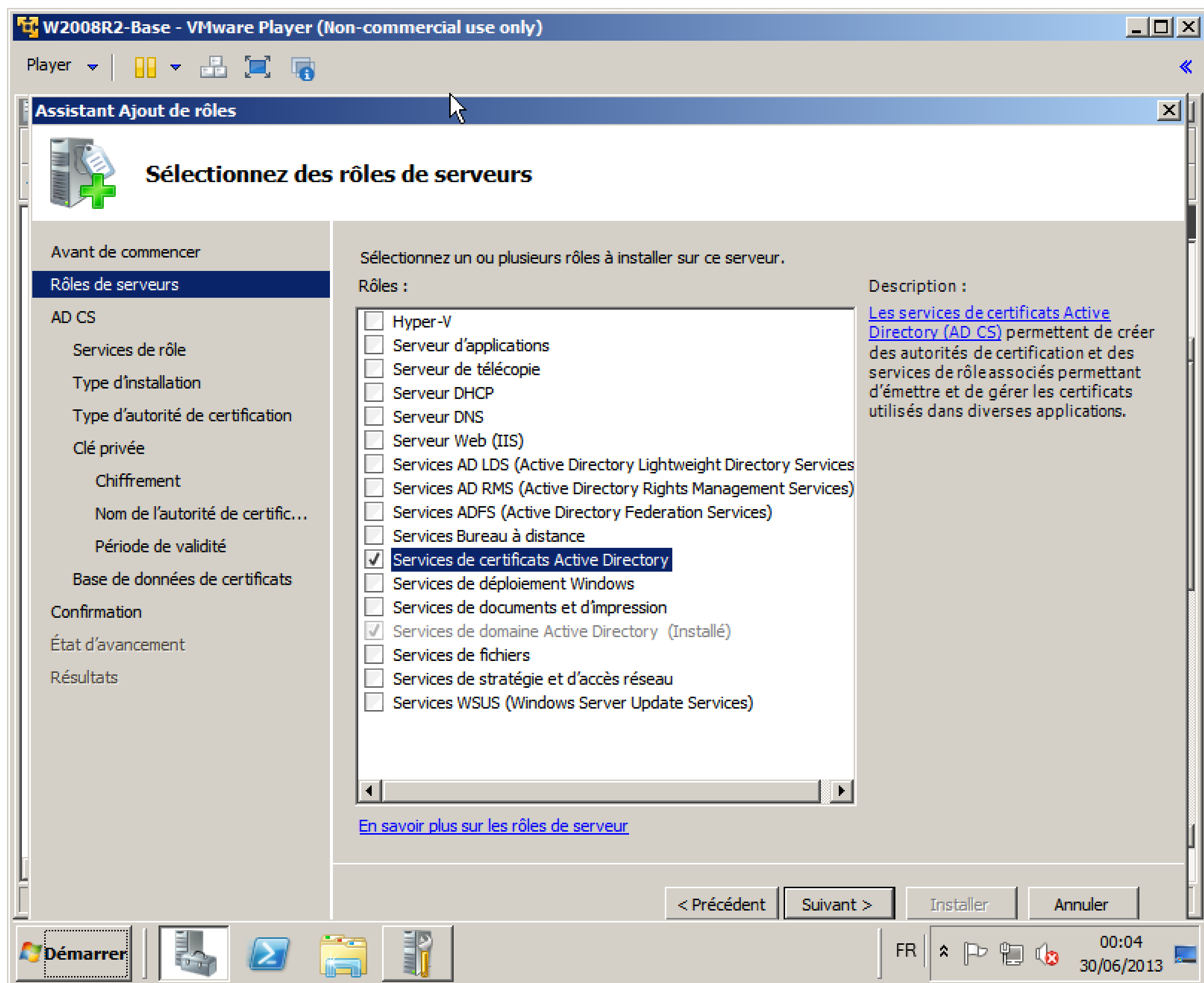


Figure 58 : AD CS : Installation du rôle

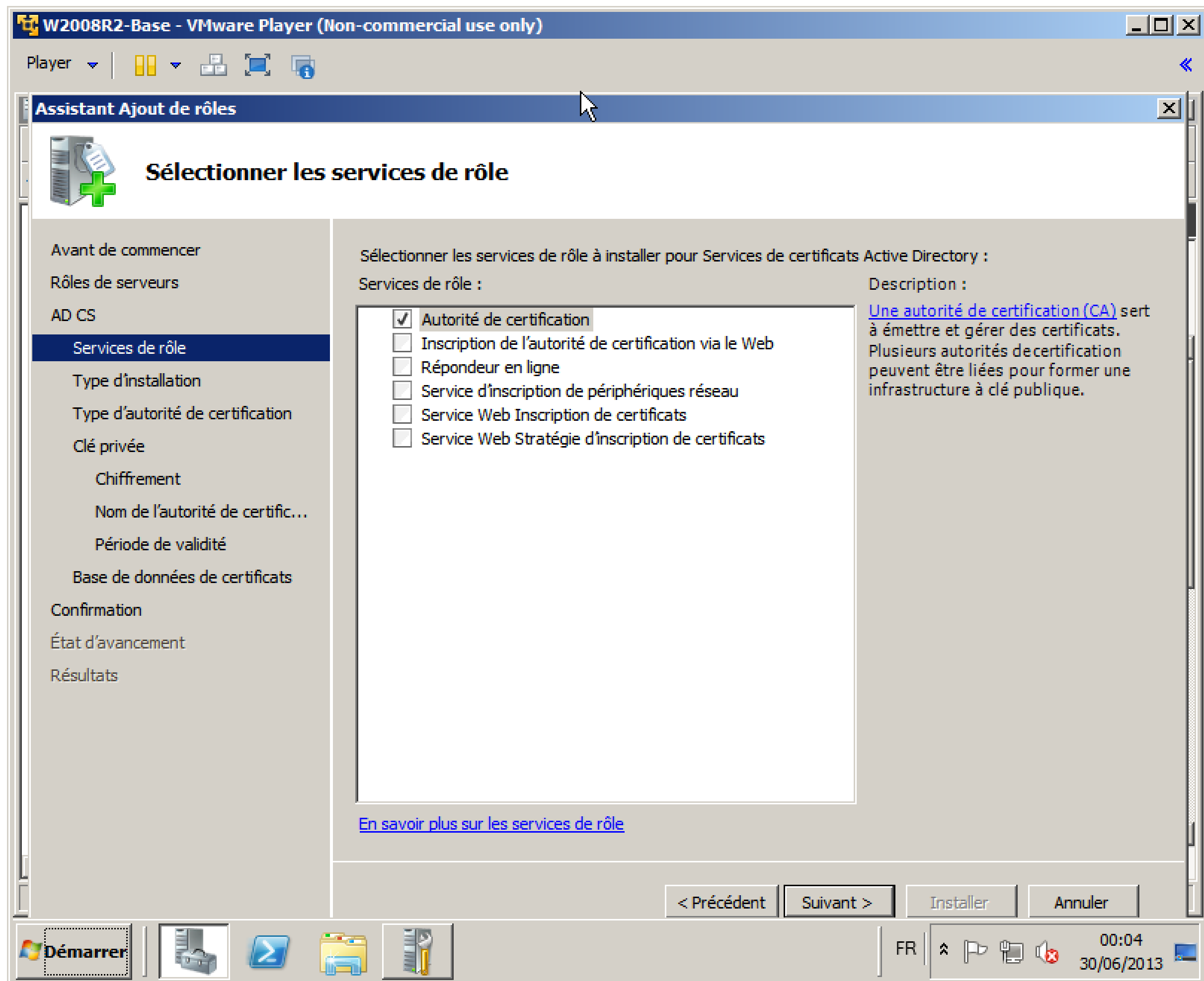


Figure 59 : AD CS : service du rôle « Autorité de certification »

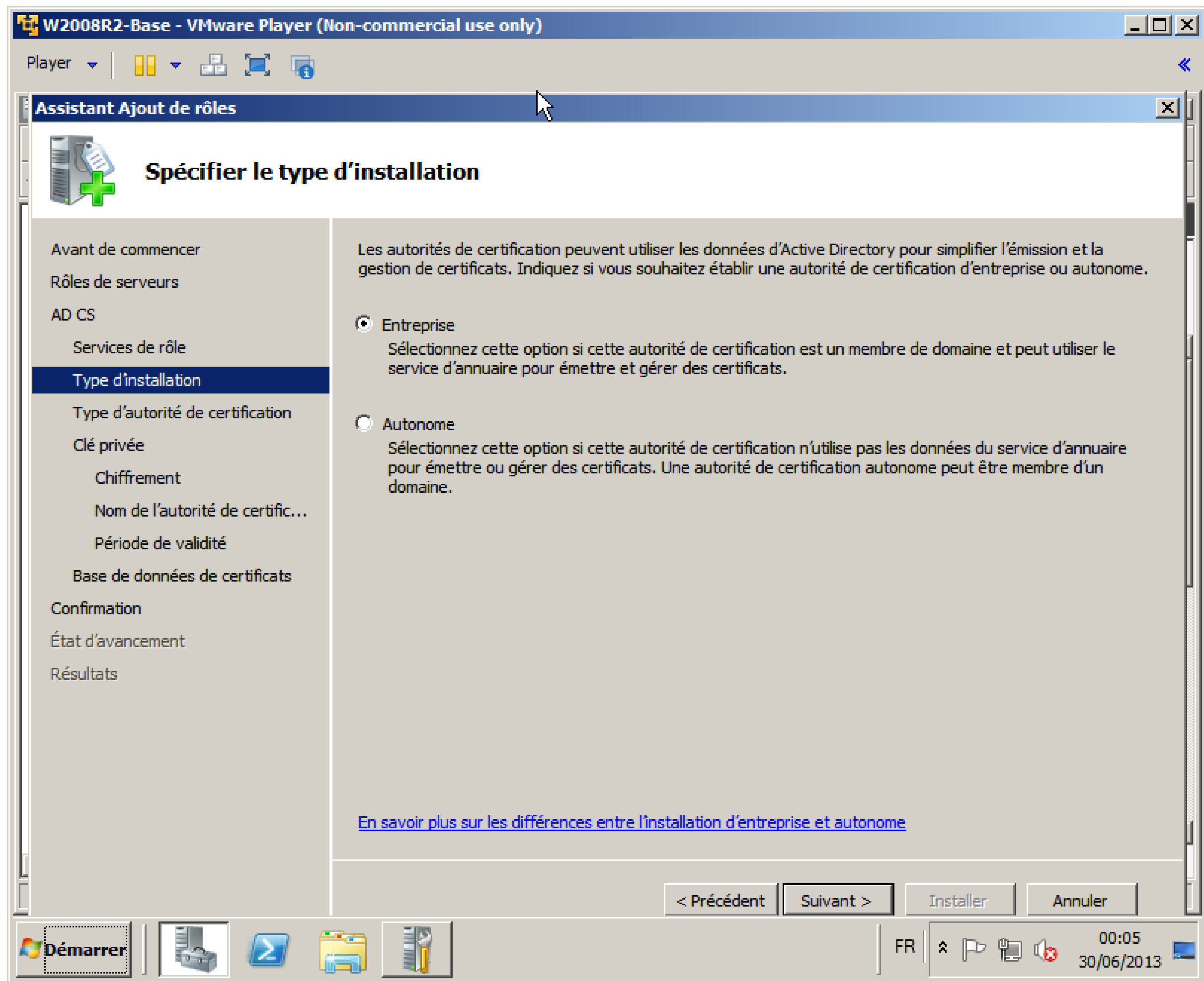


Figure 60 : AD CS : Type d'installation : Choisir « Entreprise »

Sélectionner obligatoirement « entreprise » (pour permettre la propagation automatique de cette autorité sur toutes les machines du domaine)

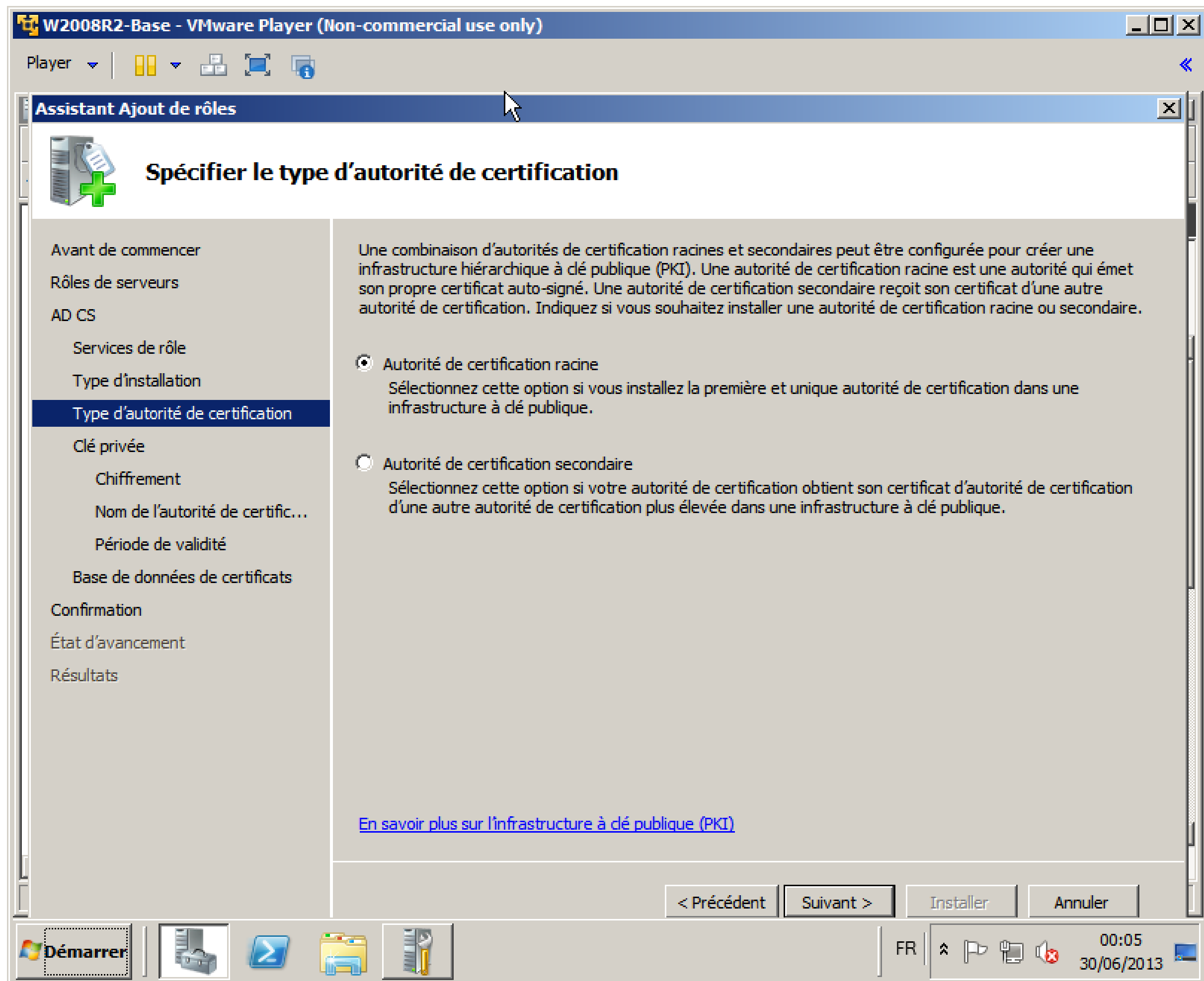


Figure 61 : AD CS : type d'autorité : Choisir « Autorité de certification racine »

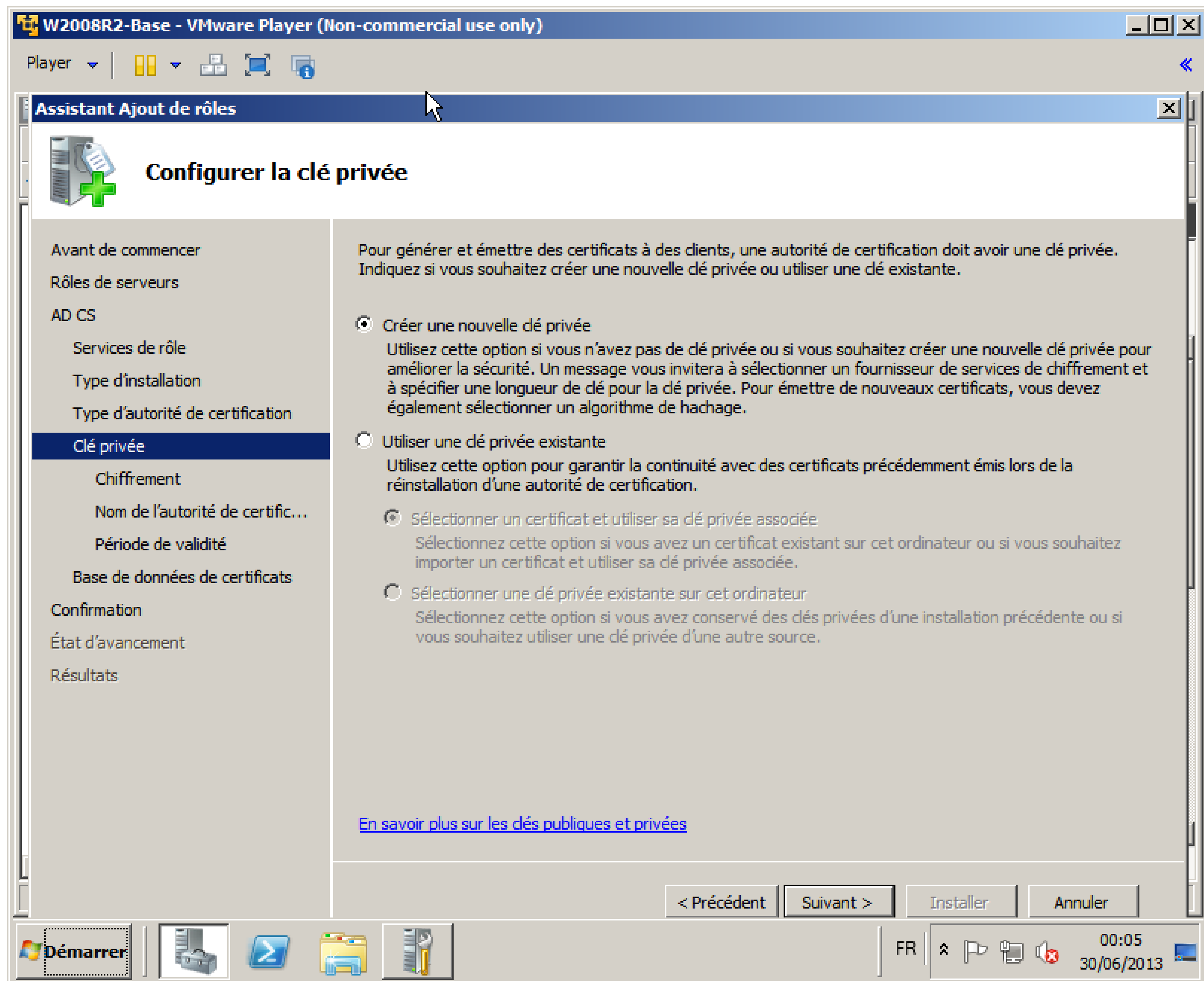


Figure 62 : AD CS : Choisir « Créer une nouvelle clé privée »

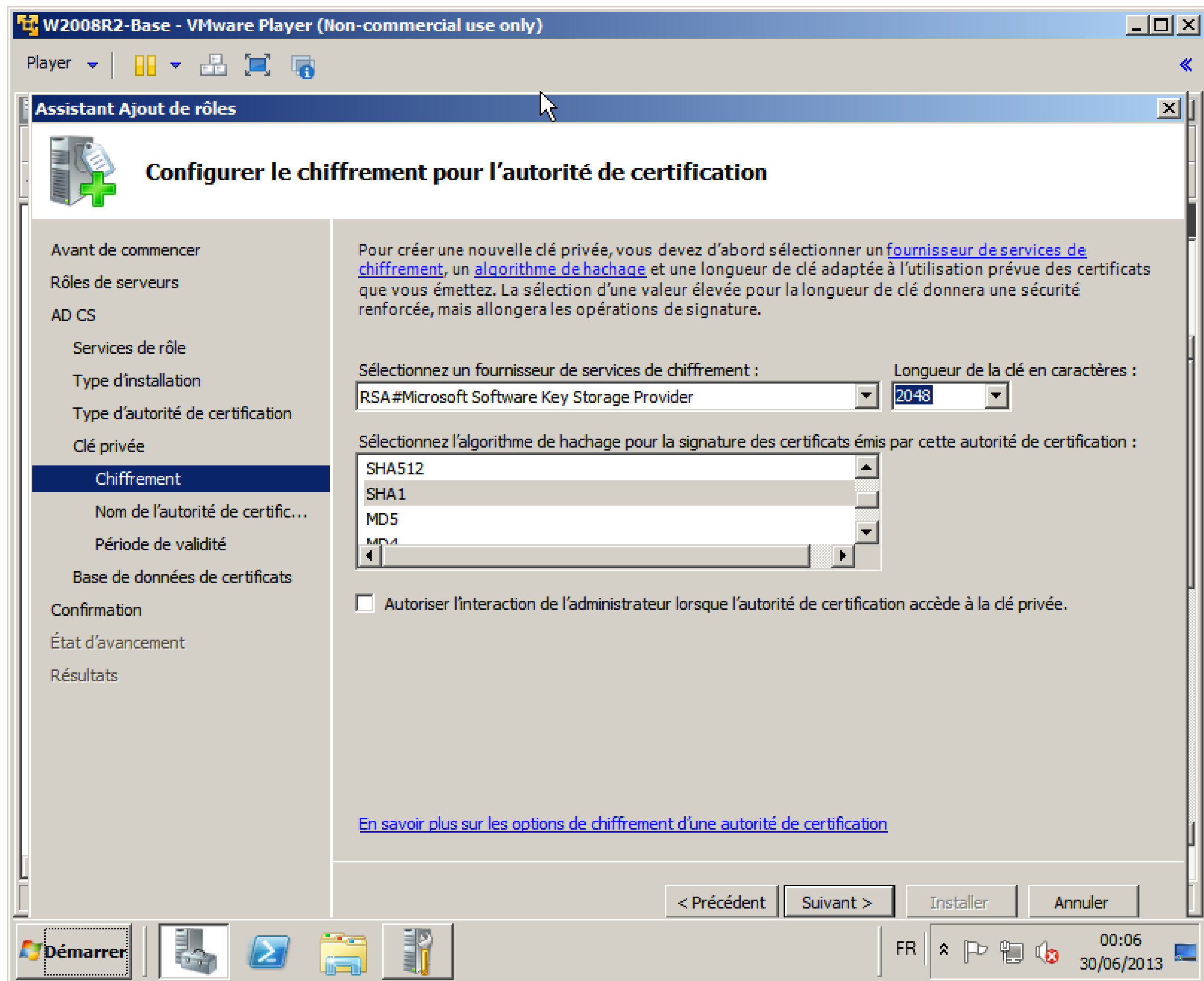


Figure 63 : AD CS : clé privée : Chiffrement

S'assurer que le choix effectué est en adéquation avec la politique de sécurité de l'environnement de production visé.

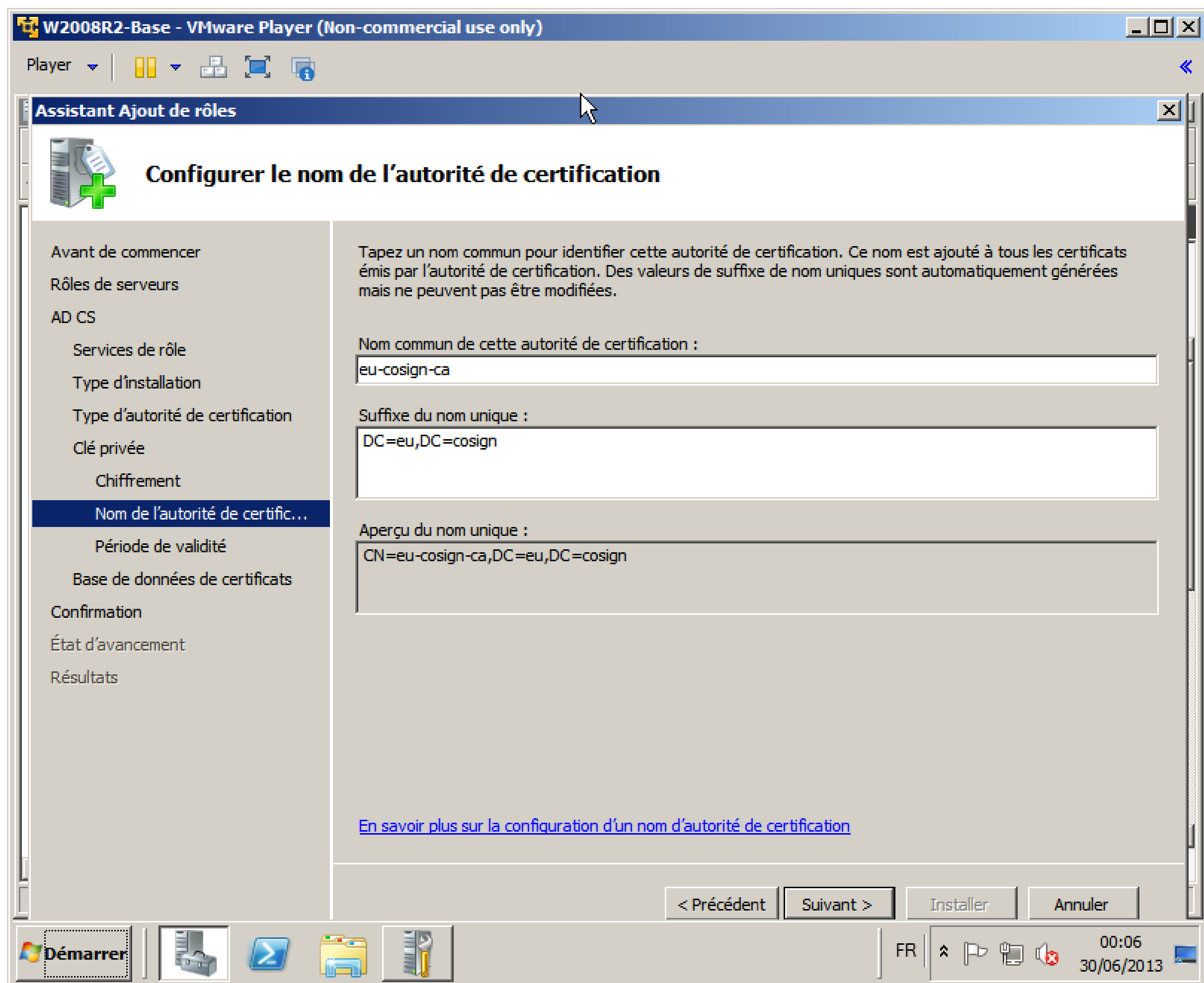


Figure 64 : AD CS : clé privée : Préciser le nom de l'AC

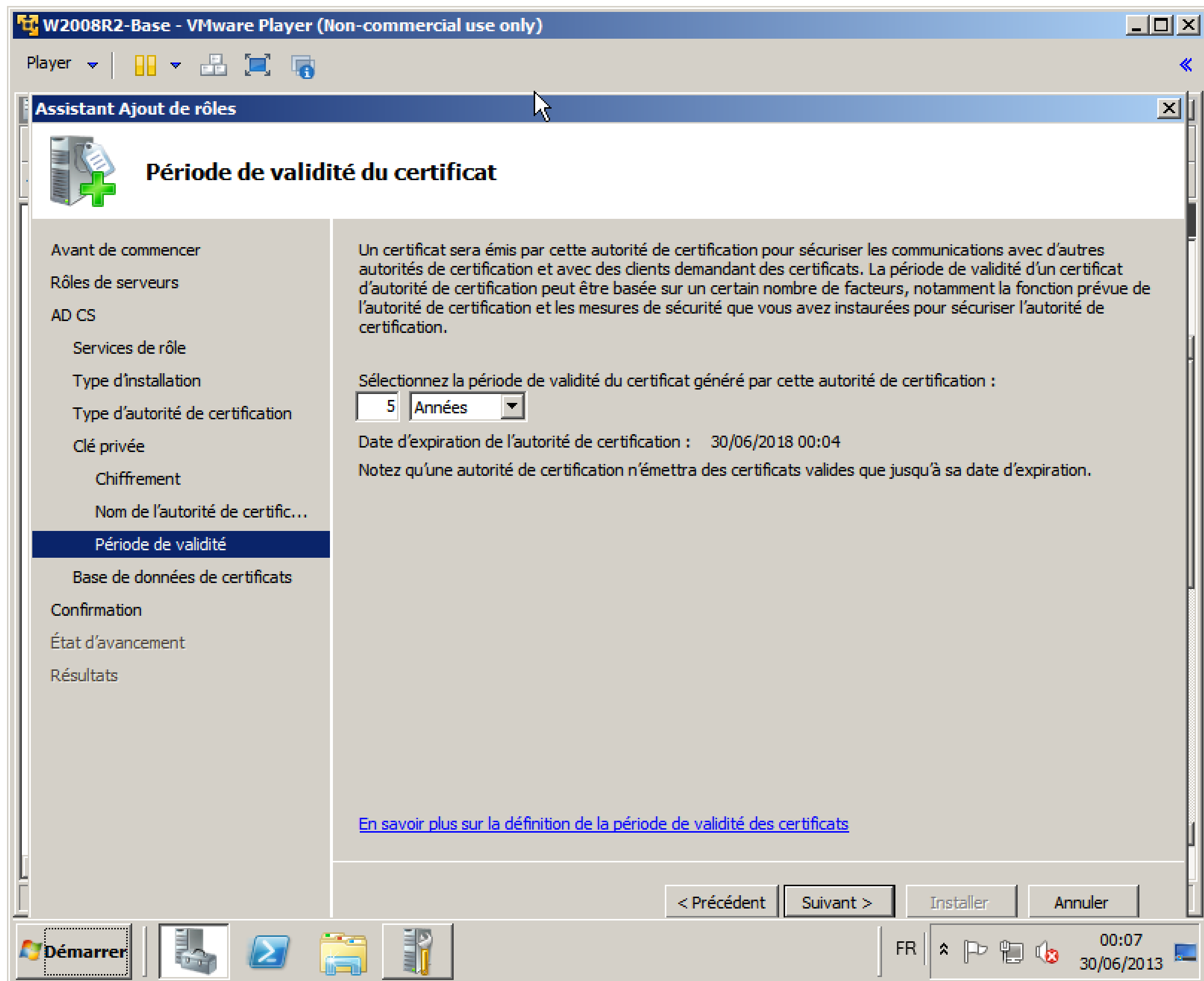


Figure 65 : AD CS : clé privée : Préciser la période de validité

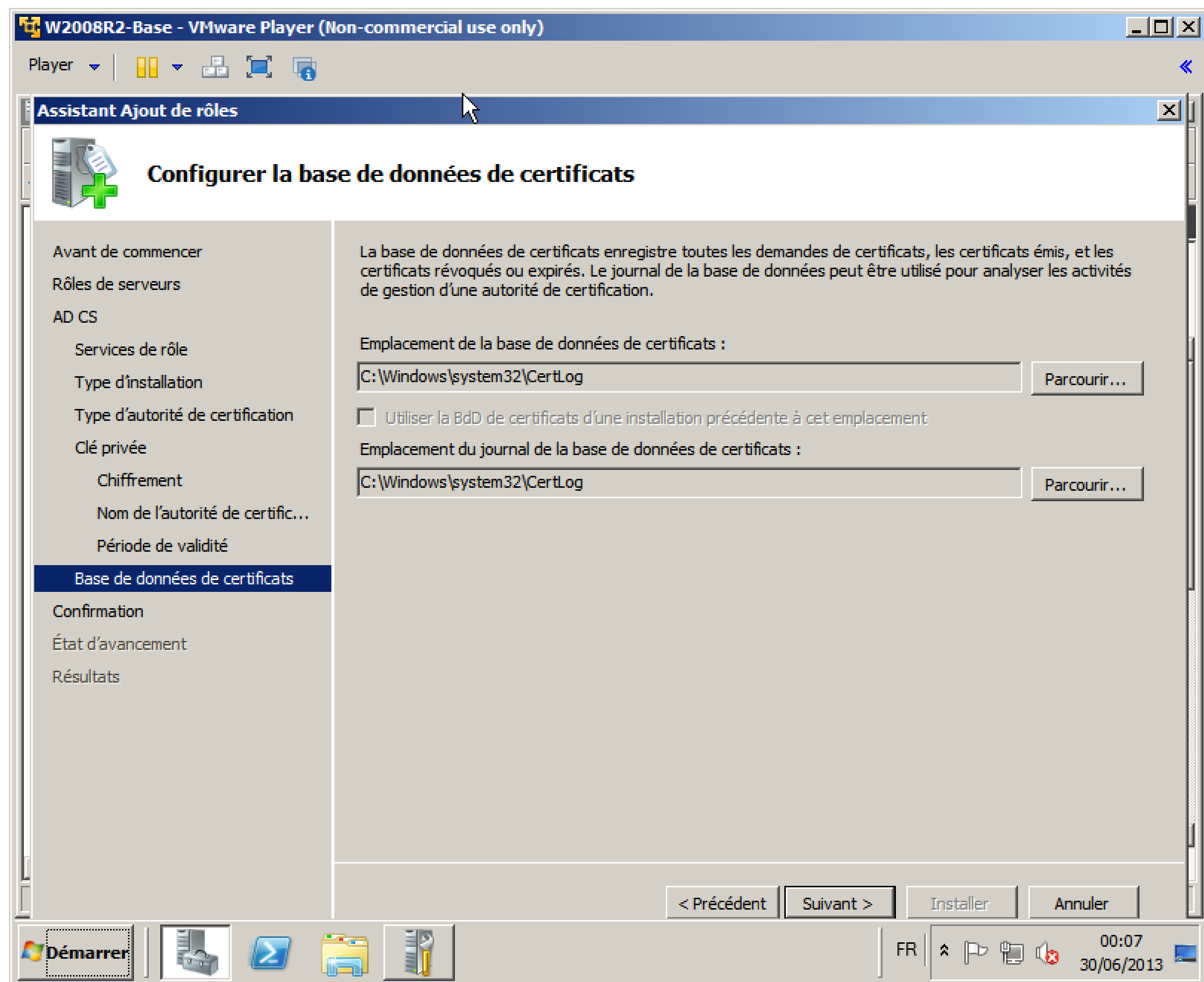


Figure 66 : AD CS : clé privée : Base de données de certificats

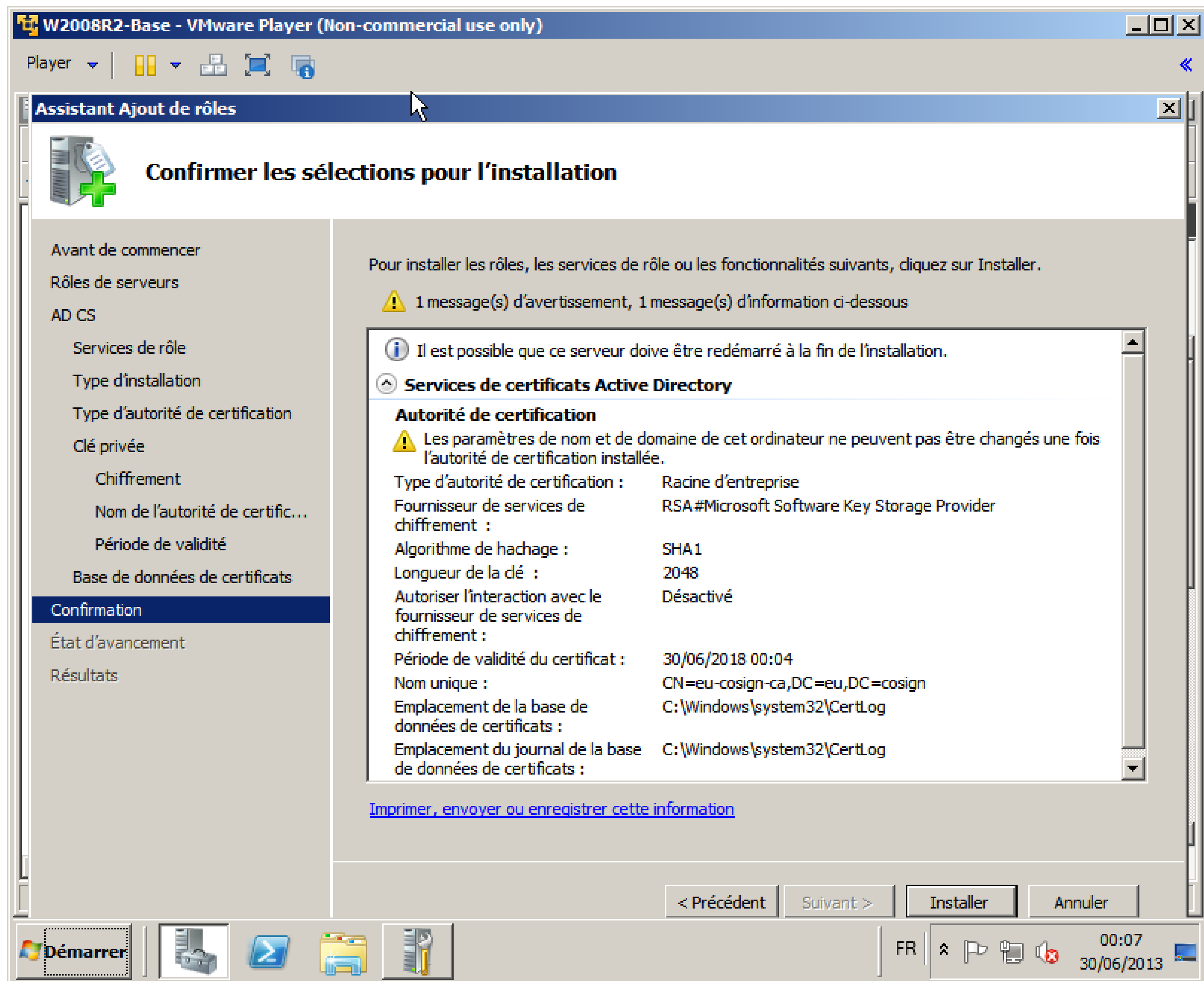


Figure 67 : AD CS : clé privée : confirmation

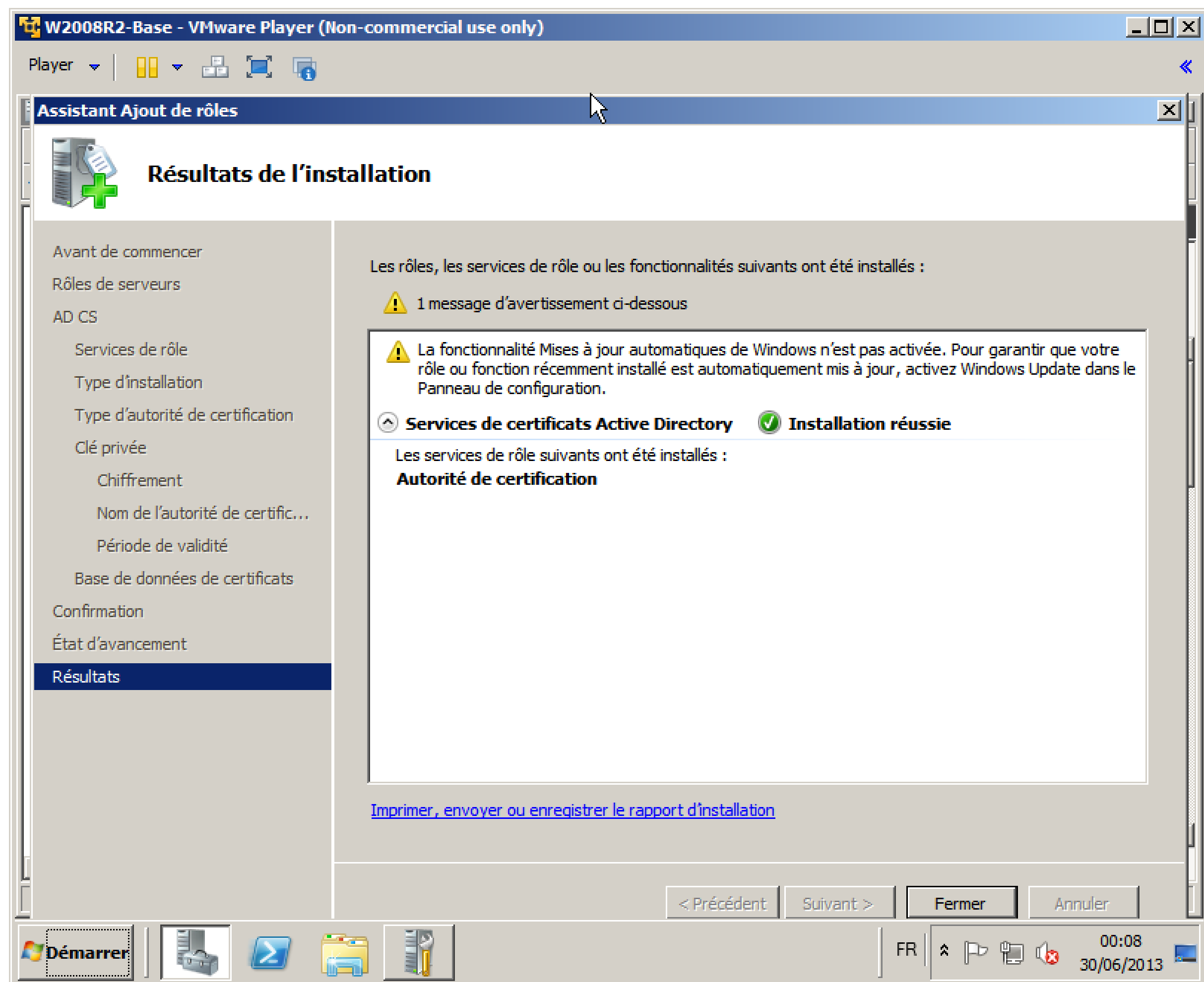


Figure 68 : AD CS : clé privée : résultats

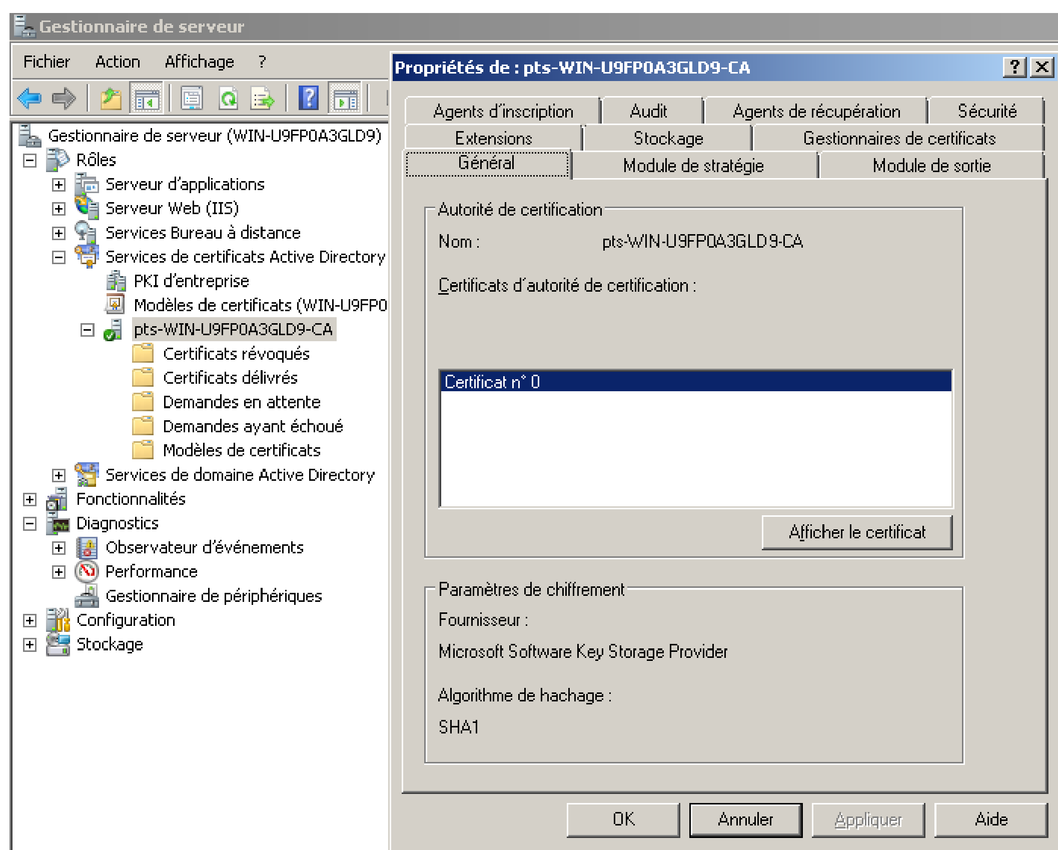


Figure 69 : AD CS: Certificat AD CS

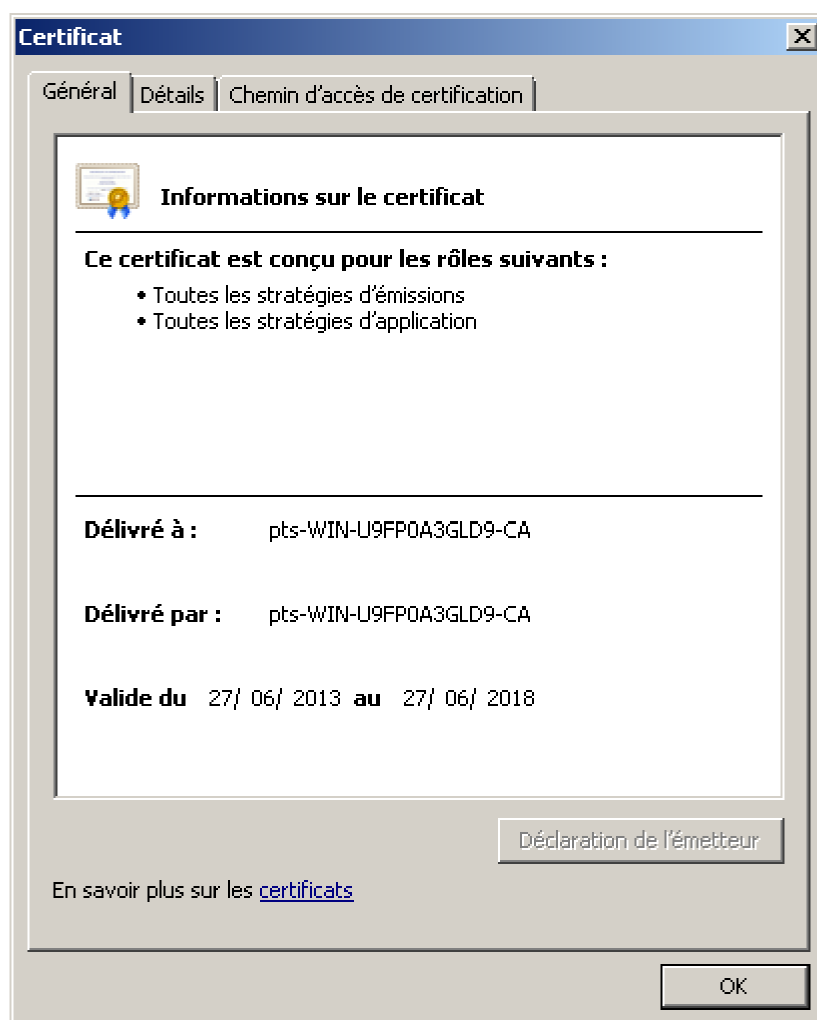


Figure 70 : AD CS: Certificat AD CS

Conseil: exporter ce certificat dans un fichier %USERPROFILE%\Desktop**ad-cs-rootca.cer**

Rebooter le Domain Controller.

Une fois que le Domain Controller a rebooté, le certificat délivré par l'AD CS au Domain Controler apparaît dans le liste des certificats délivrés par l'AD CS :

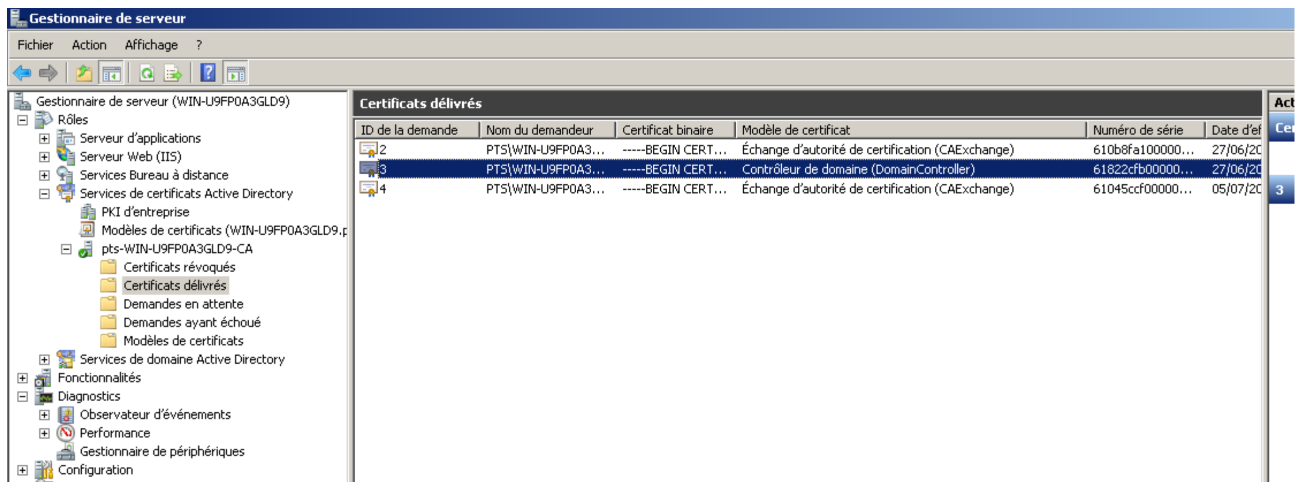


Figure 71 : AD: Certificat AD deliver par AD CS

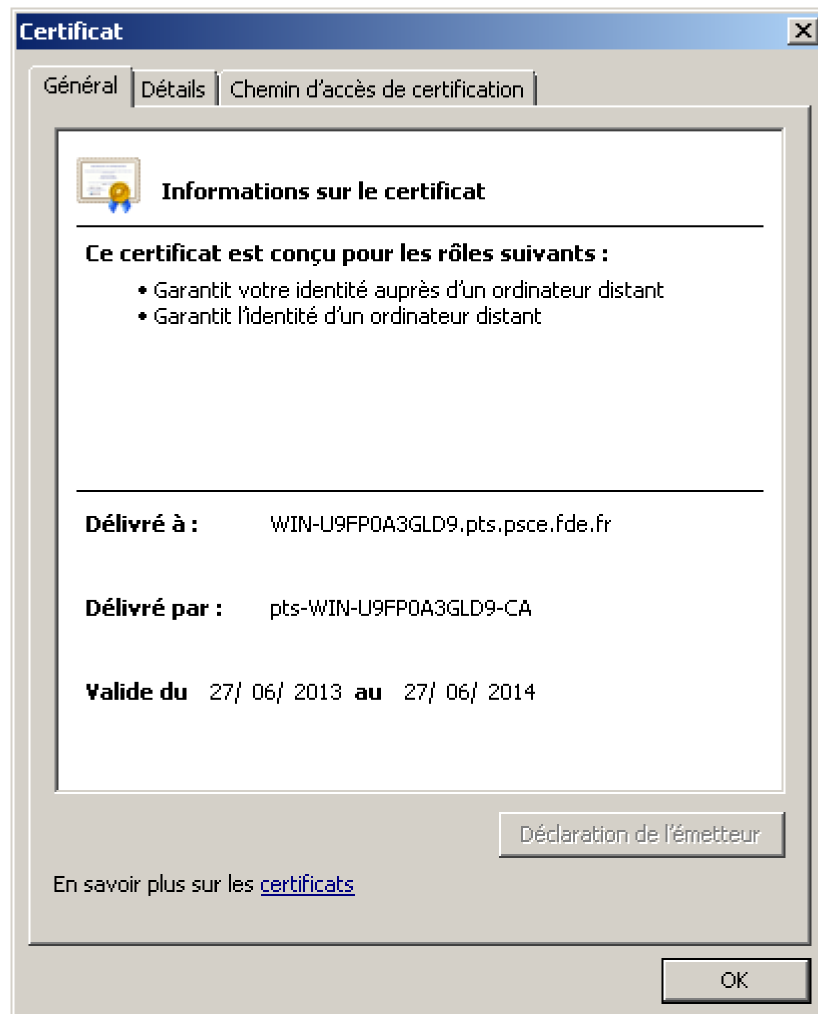


Figure 72 : AD: Certificat AD DomainController délivré par AD CS

Conseil: exporter ce certificat dans un fichier %USERPROFILE%\Desktop**ad-dc-rootca.cer**

Sur un SI en production, l'autorité racine (ACR) ne doit pas délivrée de certificats end-user directement : on préférera créer une autorité intermédiaire (ACI) qui le fera.

Le rôle AD CS est critique dans ce type de système. Se posent en particulier les questions de continuité de service en cas de défaillance de la machine hébergeant ce service ou d'expiration des certificats d'ACRR ou d'ACI.

En production, il faut donc prévoir une sauvegarde de ces environnements et éventuellement de mettre en œuvre le séquestre Microsoft (KRA – Key Recovery Agent).

12.6 Installation d'un rôle Terminal Server

12.6.1 Installation des composants du rôle Terminal Server

Terminal Server s'installe en ajoutant le rôle « **Service de bureau à distance** ». Le serveur doit rebooter à la fin de l'installation du rôle.

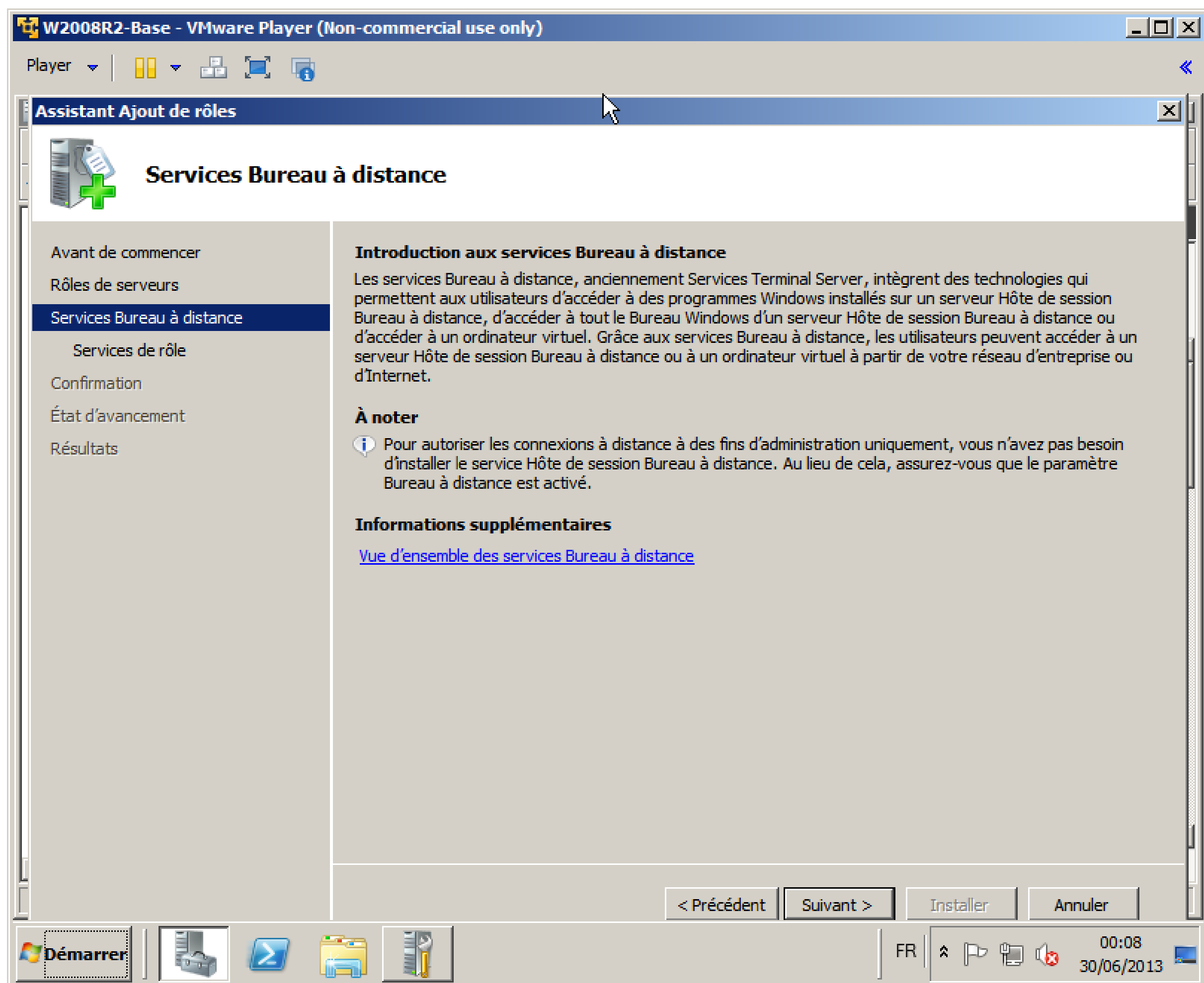


Figure 73 : Terminal Server : installation du rôle

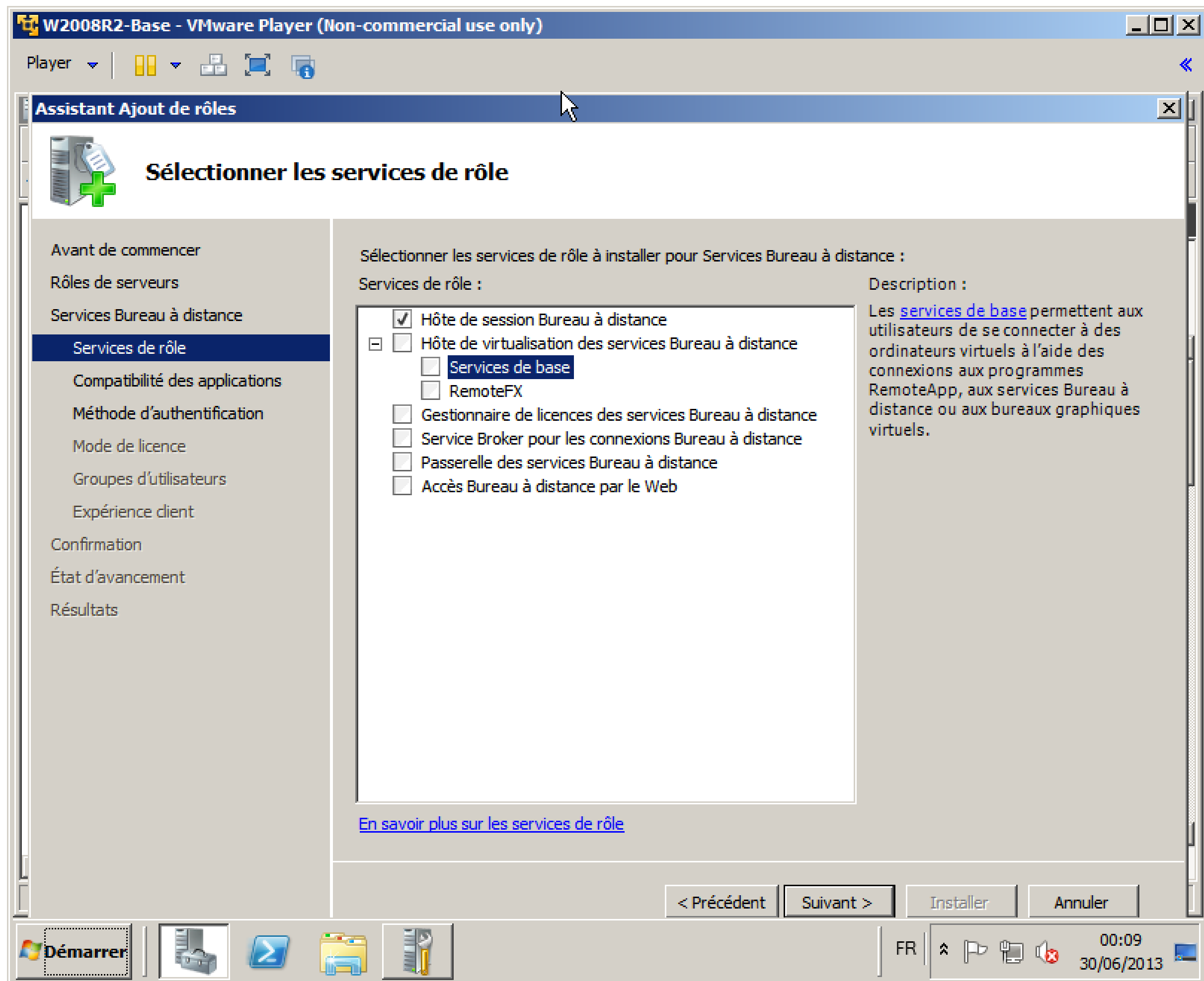


Figure 74 : Terminal Server : service de rôle : choisir « Hôte de session Bureau à distance »

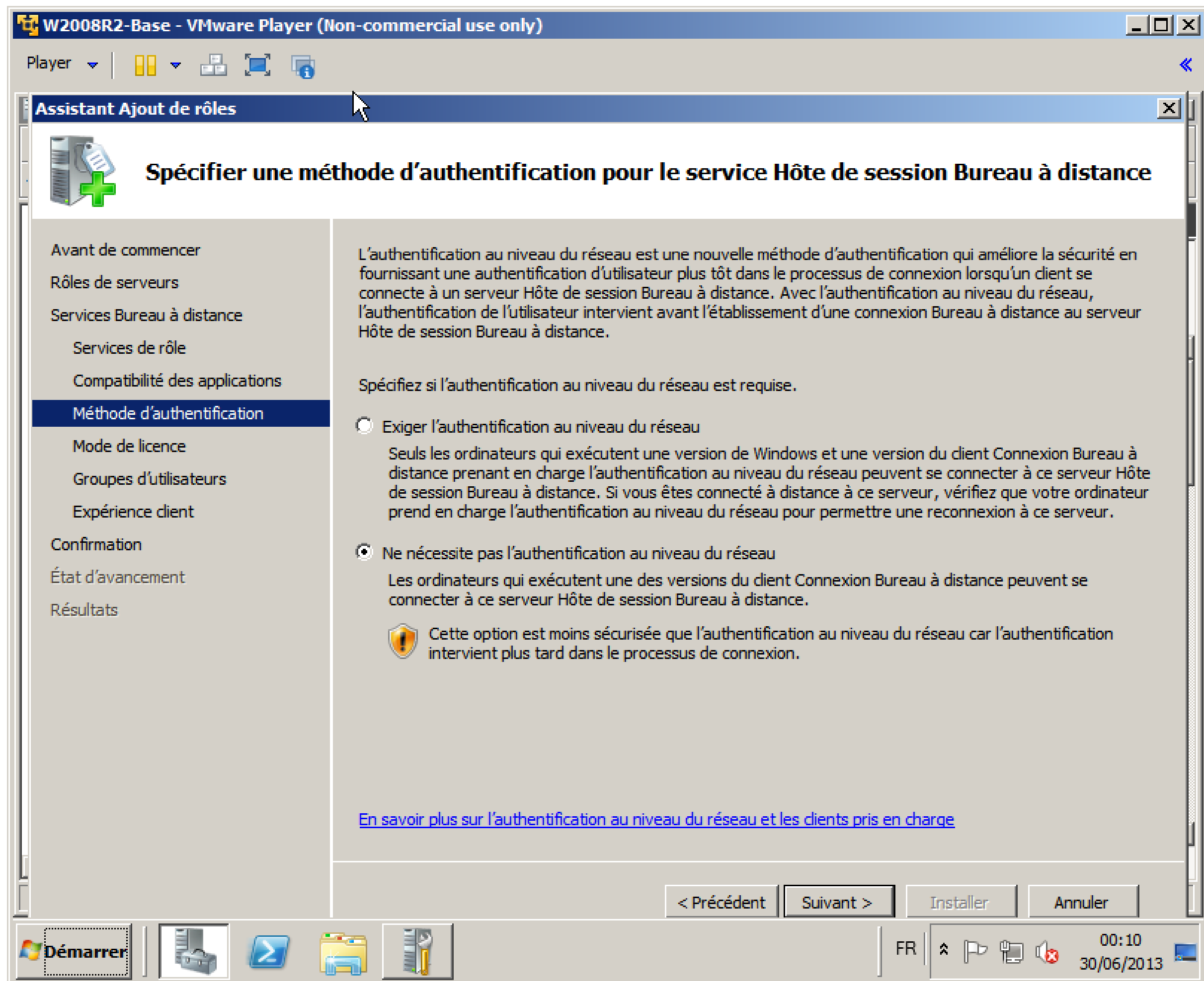


Figure 75 : Terminal Server : mode d'authentification RDP : Choisir « Ne nécessite pas l'authentification au niveau réseau »

« L'authentification au niveau réseau » est une fonctionnalité récente des serveurs RDP Microsoft. Des tests sont en cours pour vérifier que les Cryptolib CPS supportent ce mode en Smartcard logon.

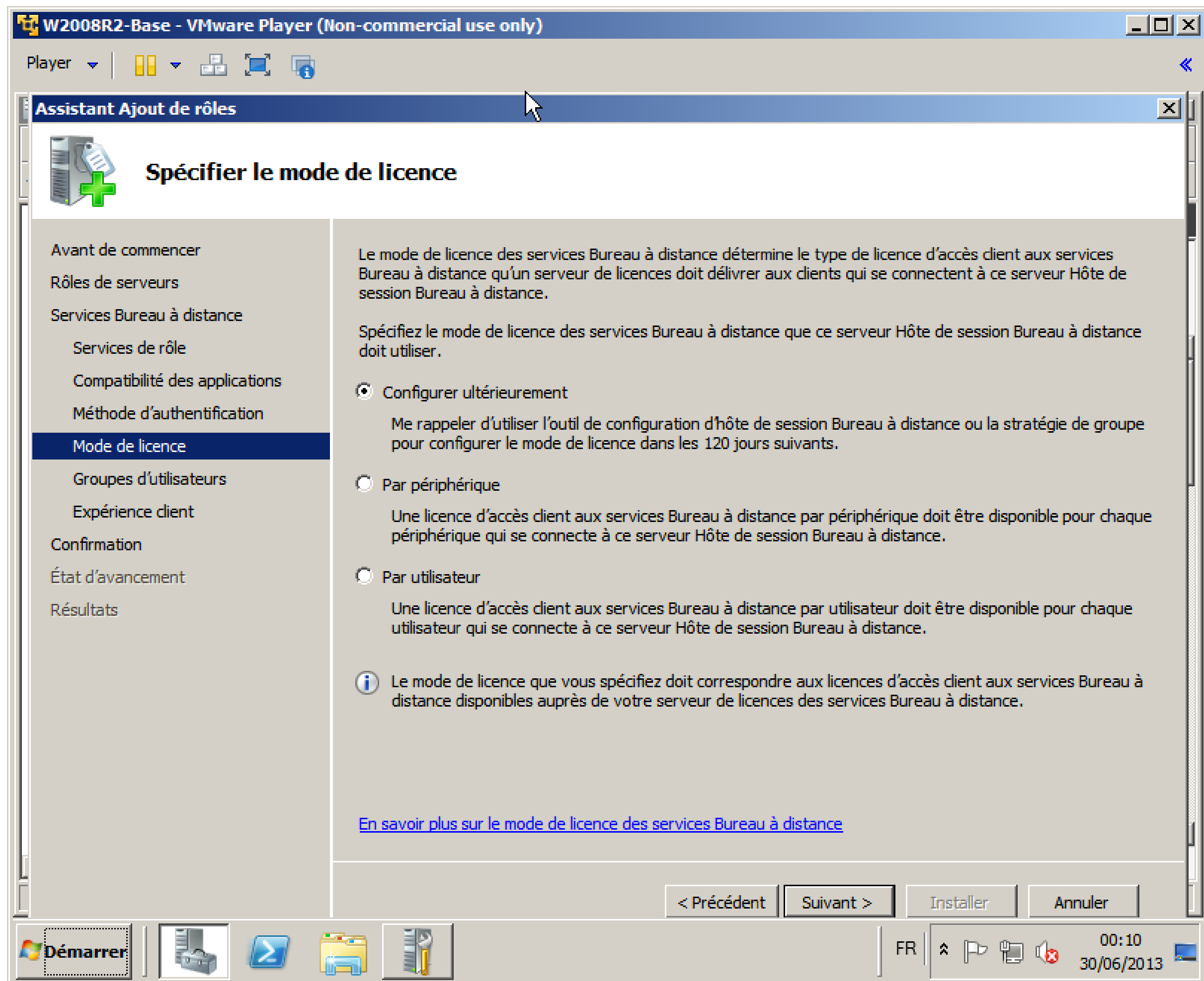


Figure 76 : Terminal Server : mode de licence : Choisir « Configurer ultérieurement »

L'activation et l'installation des licences RDP doit faire l'objet d'une attention particulière. Elle n'est pas « urgente ». Même si elle n'est pas effectuée, des tests sont possibles. Cf. ci-après.

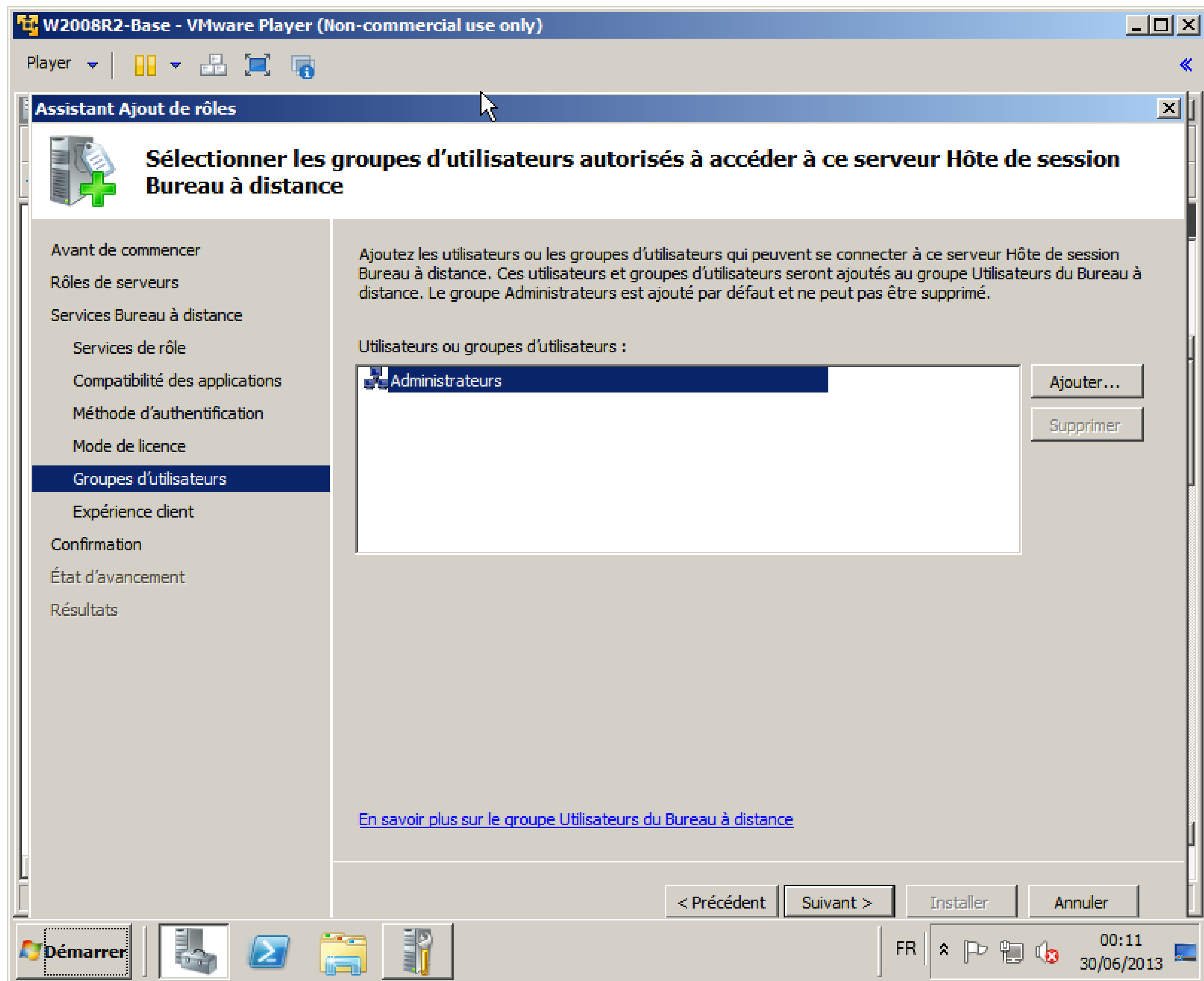


Figure 77 : Terminal Server : utilisateurs : garder « Administrateurs »

Il conviendra d'ajouter le groupe « Utilisateurs de bureau à distance » plus tard dans la configuration du serveur (cf. ci-après).

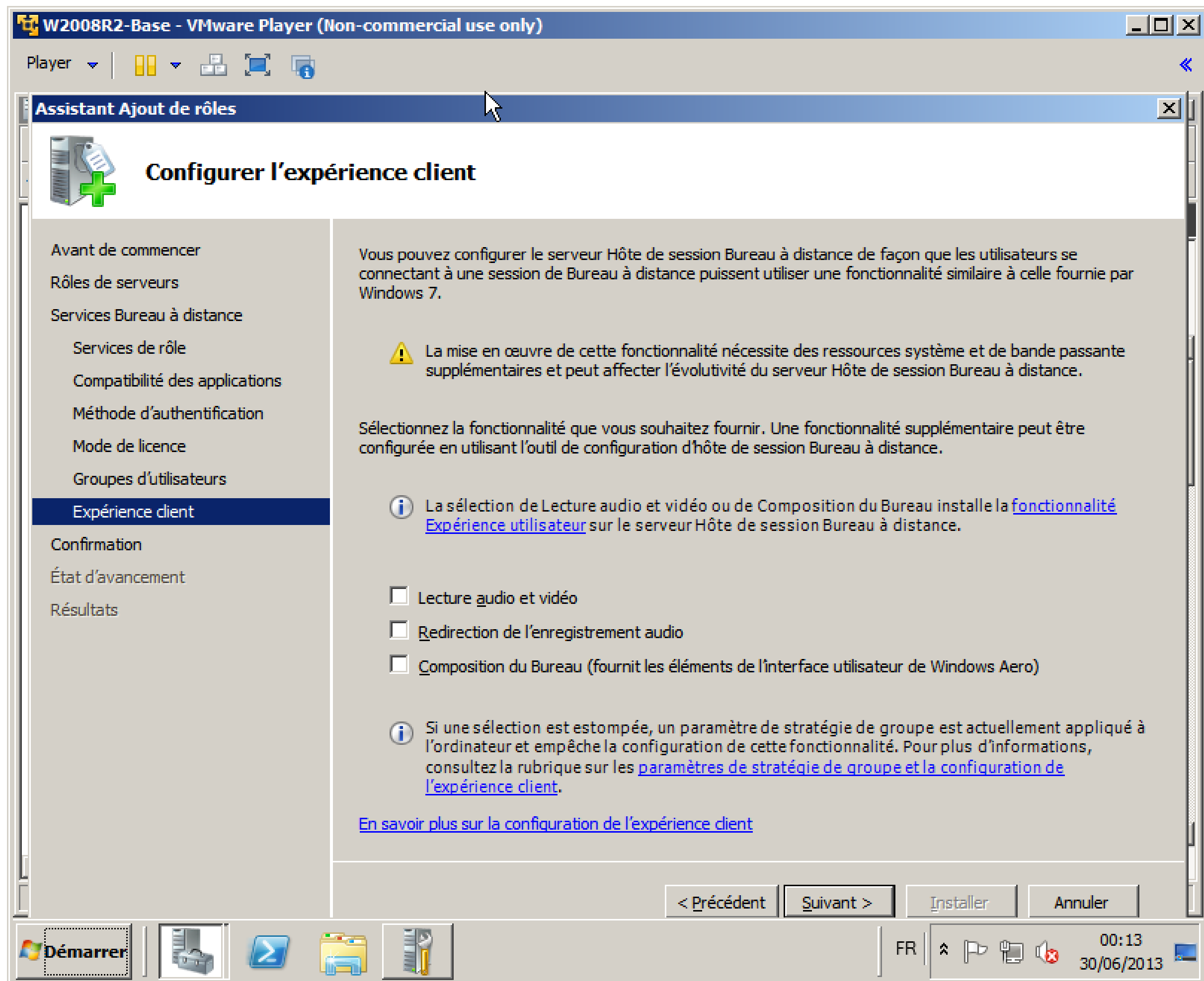


Figure 78 : Terminal Server : expérience client

Un reboot est nécessaire.

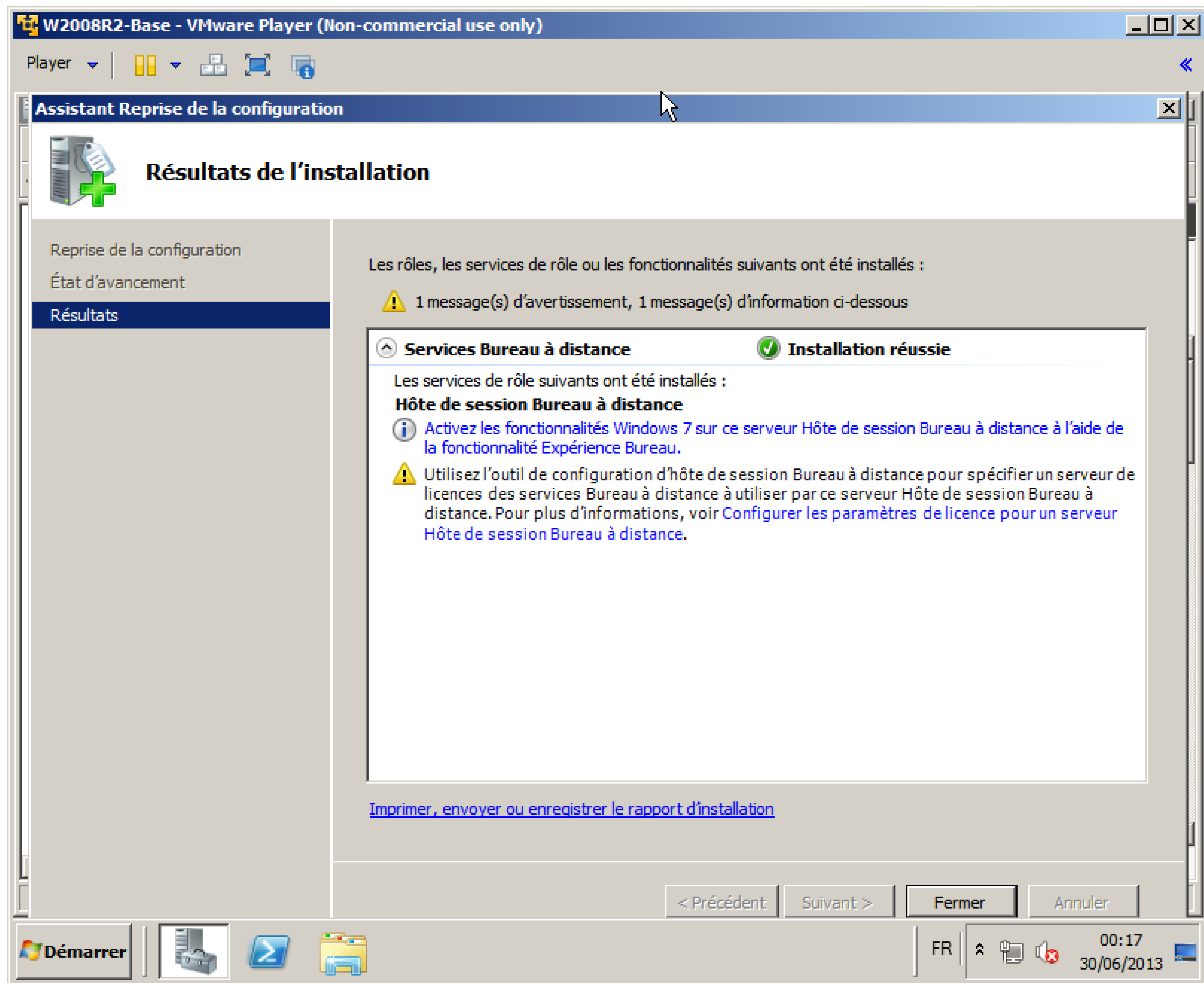


Figure 79 : Terminal Server : résultat de l'installation

12.6.2 Activation du serveur de licence RDP

Une fois le rôle installé, il faut activer le serveur de licences RDP via le **Gestionnaire des licences des services Bureau à distance.** Cette activation est gratuite. Elle se fait auprès de Microsoft. Elle peut se faire ultérieurement.

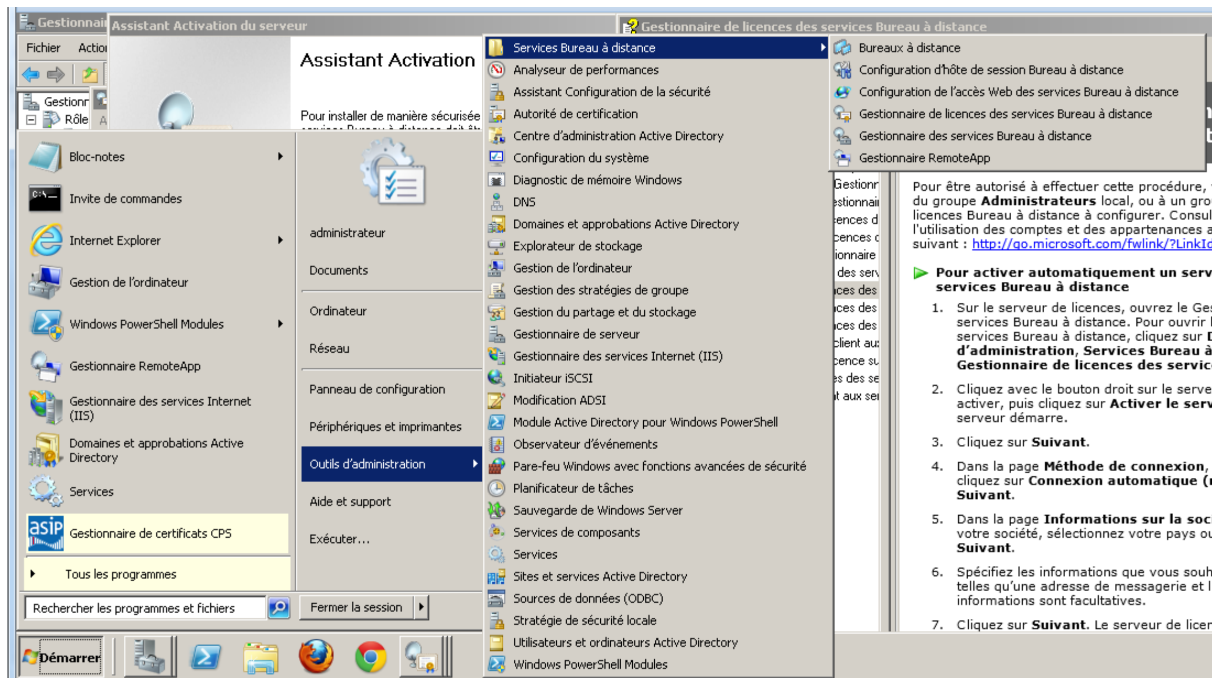


Figure 80 : Terminal Server : Lancer le Gestionnaire des licences des services Bureau à distance

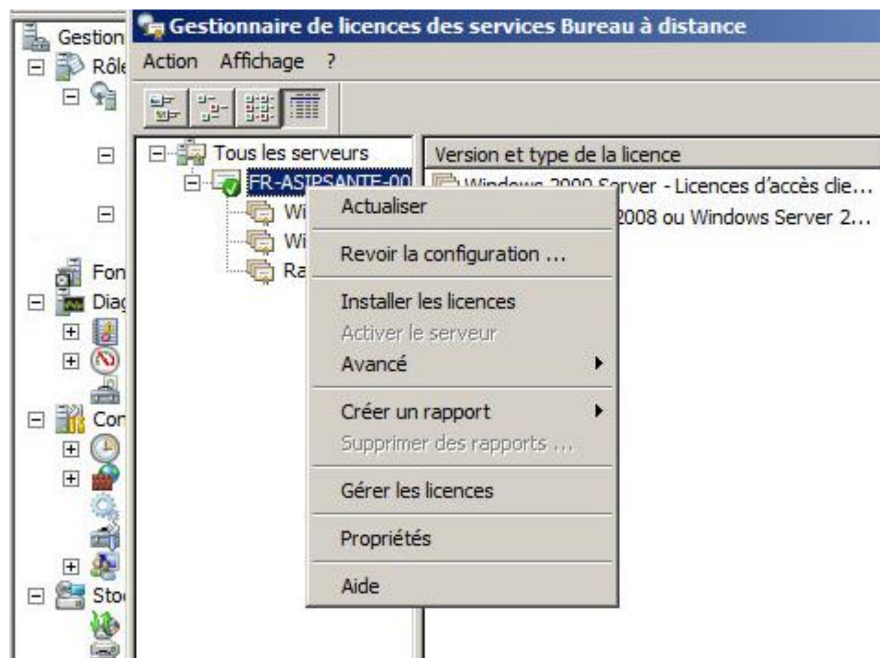


Figure 81 : Terminal Server : Clic-droit > propriétés

Préciser les propriétés du serveur de licences :

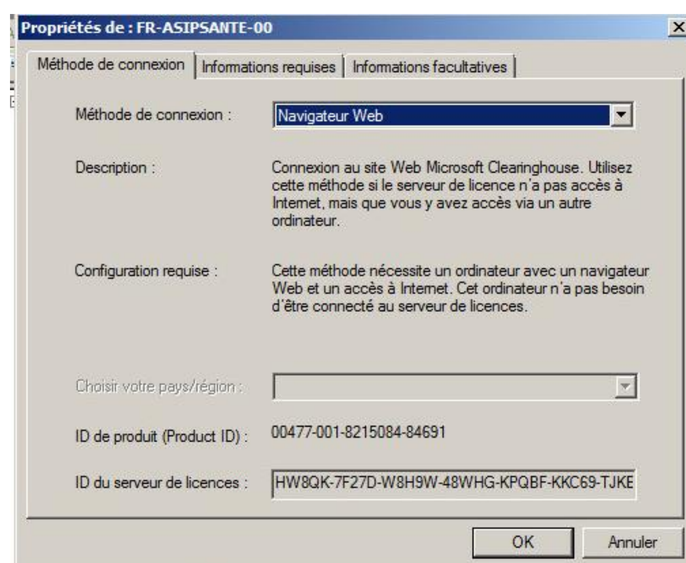


Figure 82 : Terminal Server : Mode de connexion > Navigateur Web

Puis choisir « **Activer le serveur** » (griser en figure 81).

Le serveur peut être réactivé (clic-droit > avancé > Réactivé le serveur).

12.6.3 Configurations des comptes « Serveurs de licences des services Terminal Serveur »

Le compte sous lequel tourne le serveur de licences ainsi que le compte « SERVICE RESEAU » doivent faire partie du groupe « Serveurs de licences des services Terminal Serveur »

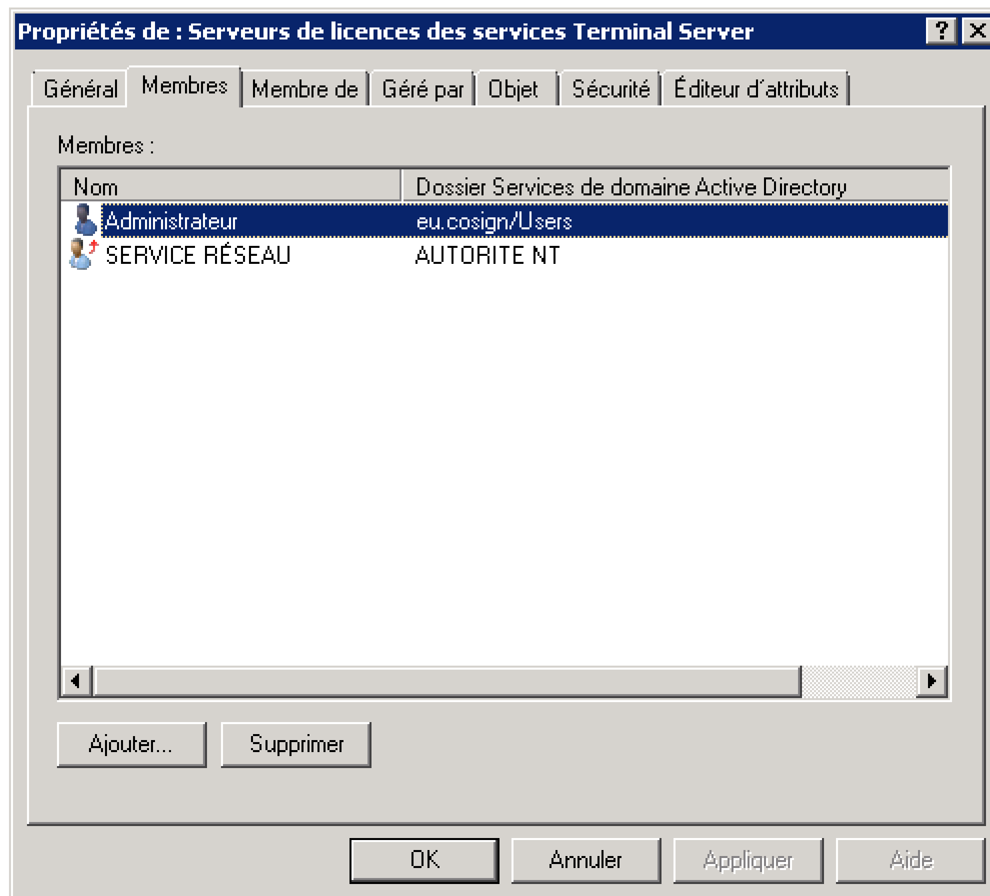


Figure 83 : Terminal Server : Configurations des comptes « Serveurs de licences des services Terminal Serveur »

12.6.4 Installation des licences sur le serveur de licences

L'installation de licences est payante. Là aussi un délai d'évaluation est accordé, ce qui permet de faire quelques tests en attendant d'acheter les licences requises (ordres d'idées : 35€ la licence CAL, 150€ le pack de 5 licences CAL, cf. Microsoft ou revendeurs, hors prix des licences serveur).
Elle peut se faire dans la foulée de l'activation du serveur de Bureau à distance ou ultérieurement par clic droit sur le serveur puis « Installer les licences ».

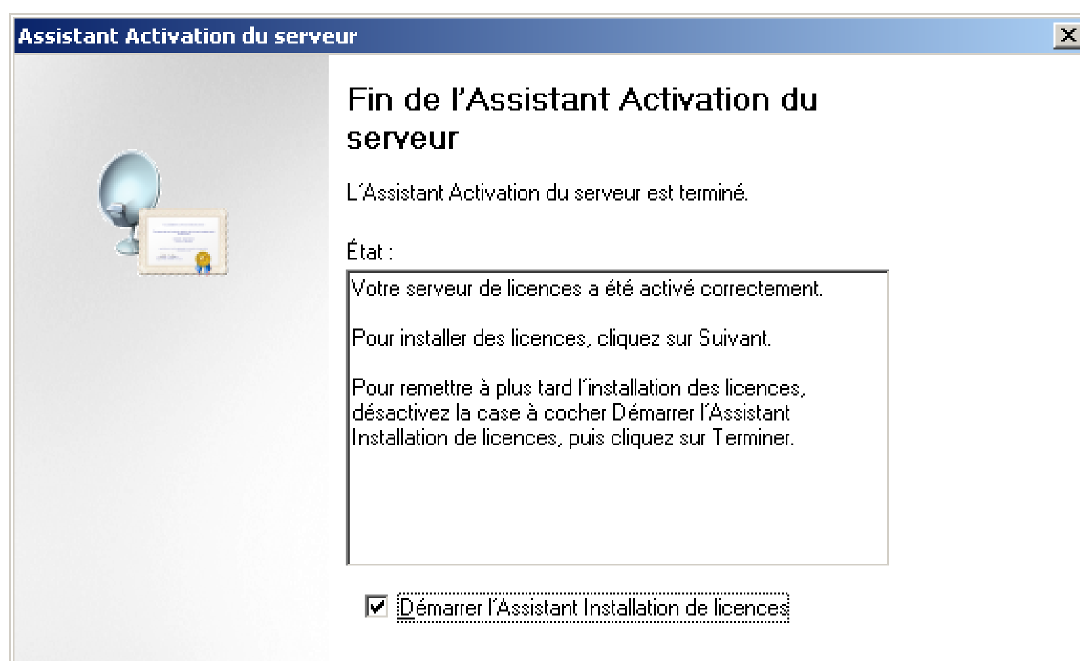


Figure 84 : Terminal Server : Fin de l'activation du serveur de licences Terminal Serveur

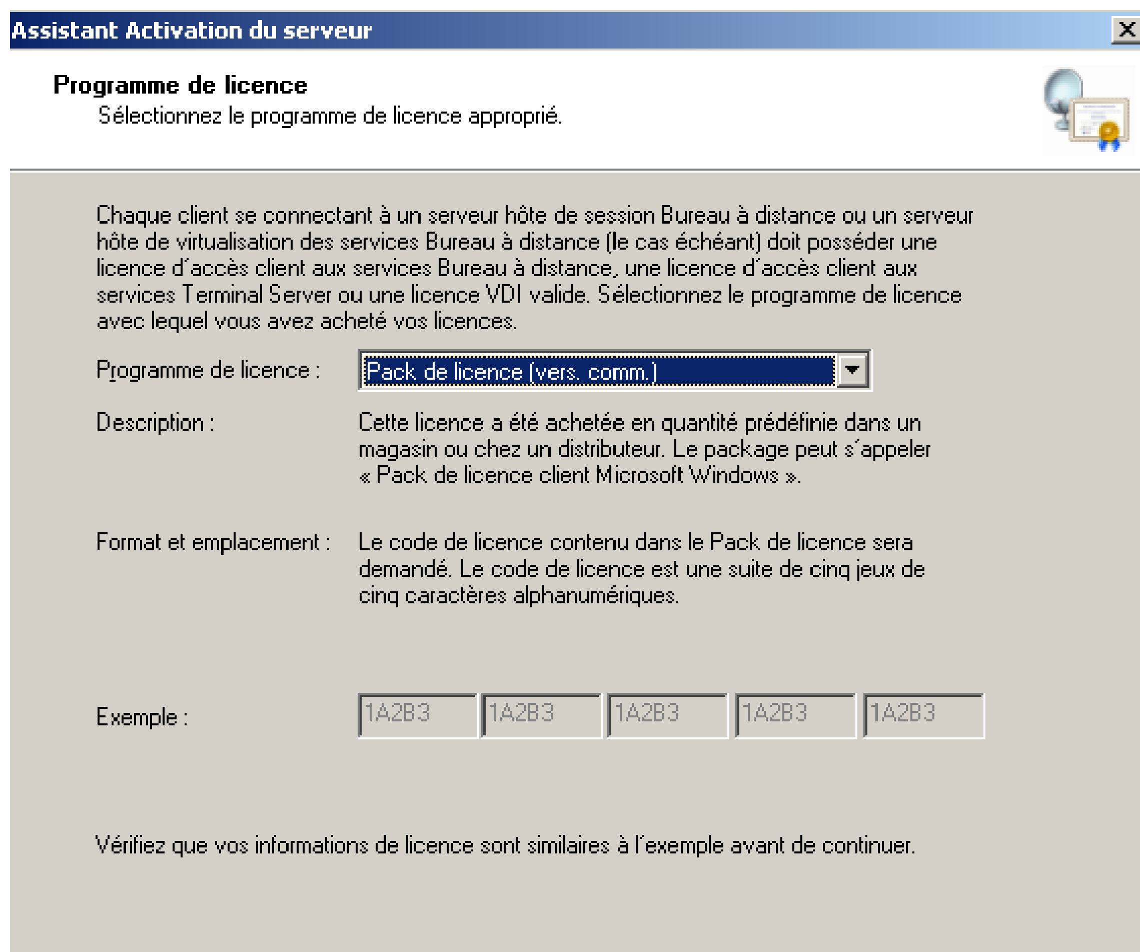


Figure 85 : Terminal Server : Installation d'un pack de licences

12.6.5 Configuration de l'hôte Terminal Server

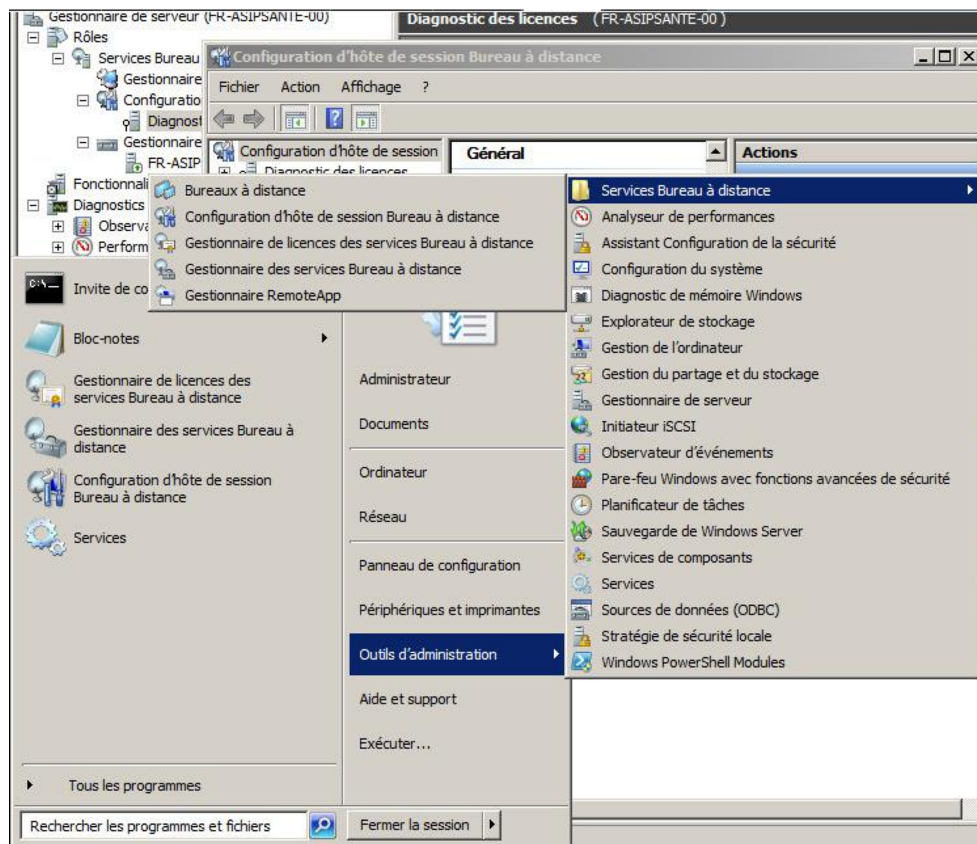


Figure 86 : Terminal Server : Configuration d'hôte de session Bureau à distance

Modifier les paramètres

Général

Supprimer les dossiers temporaires en quittant	Oui
Utiliser des dossiers temporaires par session	Oui
Restreindre chaque utilisateur à une seule ses...	Oui
Mode d'ouverture de session de l'utilisateur	Autoriser toutes les connexions

Gestionnaire de licences

Mode de licence des services Bureau à dista...	Par utilisateur
Serveurs de licences des services Bureau à d...	Spécifié

Service Broker pour les connexions Bureau à distance

Membre d'une batterie dans le service Broker ...	Non

Virtualisation IP des services Bureau à distance

Virtualisation IP	Non activé

Figure 87 : Terminal Server : Configuration d'hôte de session Bureau à distance > mode de licence et serveurs de licences

Propriétés

Service Broker pour les connexions Bureau à distance
Virtualisation IP des services Bureau à distance
Général
Gestionnaire de licences

Mode de licence des services Bureau à distance

- Non spécifié
- Par périphérique
- Par utilisateur

Serveurs de licences des services Bureau à distance

Le serveur hôte de session Bureau à distance enverra des demandes de licence d'accès client aux services Bureau à distance aux serveurs de licences spécifiés selon l'ordre dans lequel ils sont répertoriés.

Serveurs de licences spécifiés :

fr-asipsante-00

Monter
Descendre
Ajouter... Supprimer
OK Annuler Appliquer

Figure 88 : Terminal Server : Configuration d'hôte de session Bureau à distance > mode de licence et serveurs de licences

12.6.6 Paramétrage du serveur RDP

Une fois le rôle installé, le paramétrage du serveur RDP et des comptes se font de la façon suivante :

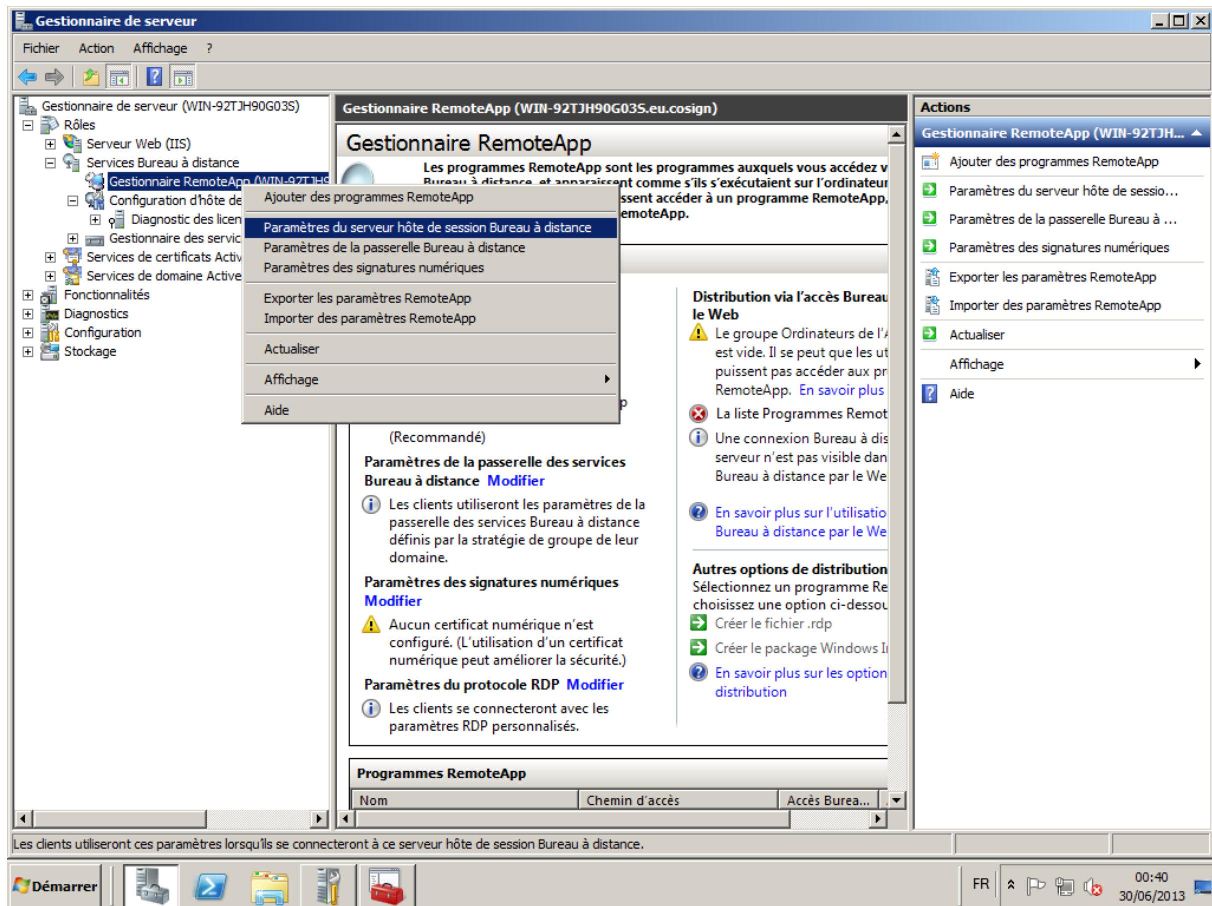


Figure 89 : Terminal Server : Configuration des paramètres serveur

Paramètres de déploiement RemoteApp

Signature numérique | Paramètres RDP communs | Paramètres RDP personnalisés

Serveur hôte de session Bureau à distance | Passerelle des services Bureau à distance

Les clients utiliseront ces paramètres lorsqu'ils se connecteront à ce serveur hôte de session Bureau à distance.

Paramètres de connexion

Nom du serveur : cosign

Si le serveur hôte de session Bureau à distance se trouve dans une batterie de serveurs, entrez le nom DNS de

Port RDP : 8389

Accès au Bureau à distance

Afficher une connexion Bureau à distance sur ce serveur hôte de session Bureau à distance dans l'accès Bureau à distance par le Web

Accéder aux programmes non listés

Ne pas permettre aux utilisateurs de démarrer les programmes non répertoriés sur la connexion initiale (Recommandé)

Permettre aux utilisateurs de démarrer les programmes répertoriés et non

OK | Annuler | Appliquer

Figure 90 : Terminal Server : config. nom du serveur et port externe

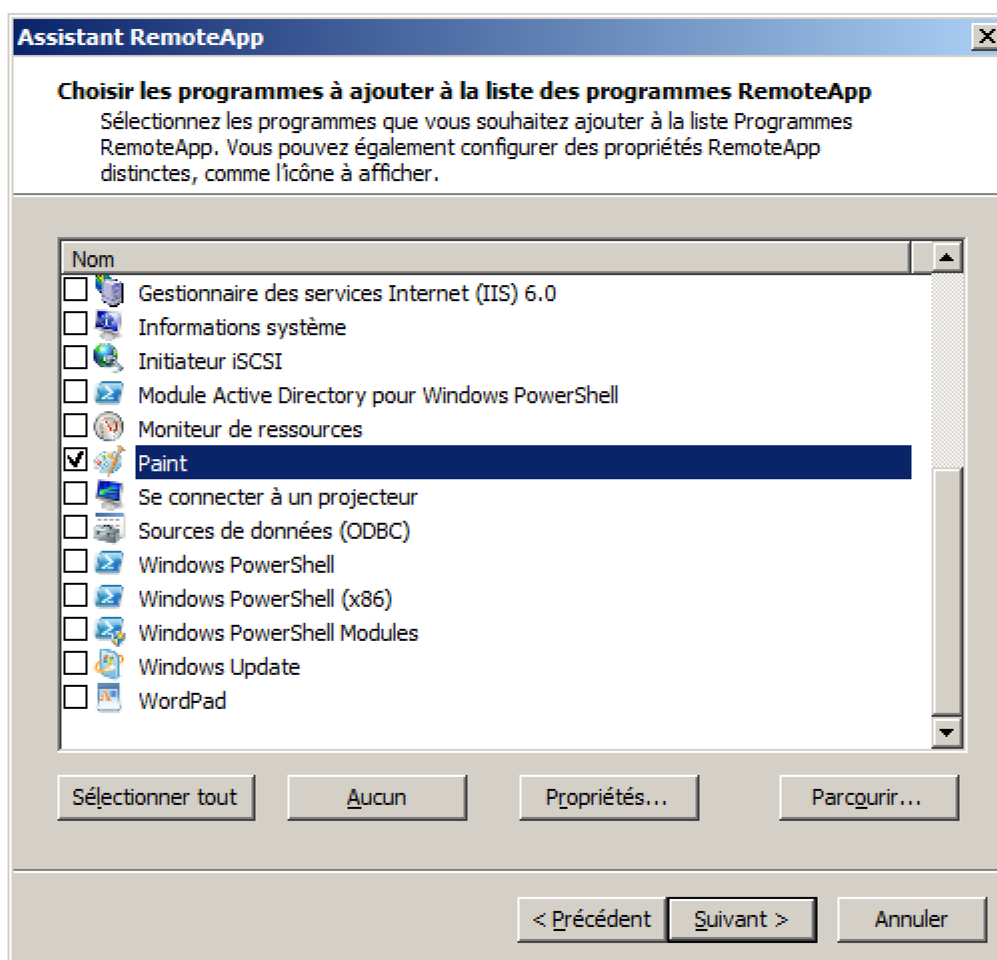


Figure 91 : Terminal Server : Déclaration d'une remote app de test

Démarrer, click **Exécuter…**, « **cmd** » puis entrer "**control system", « Paramètres système avancés », « Utilisation à distance » :**

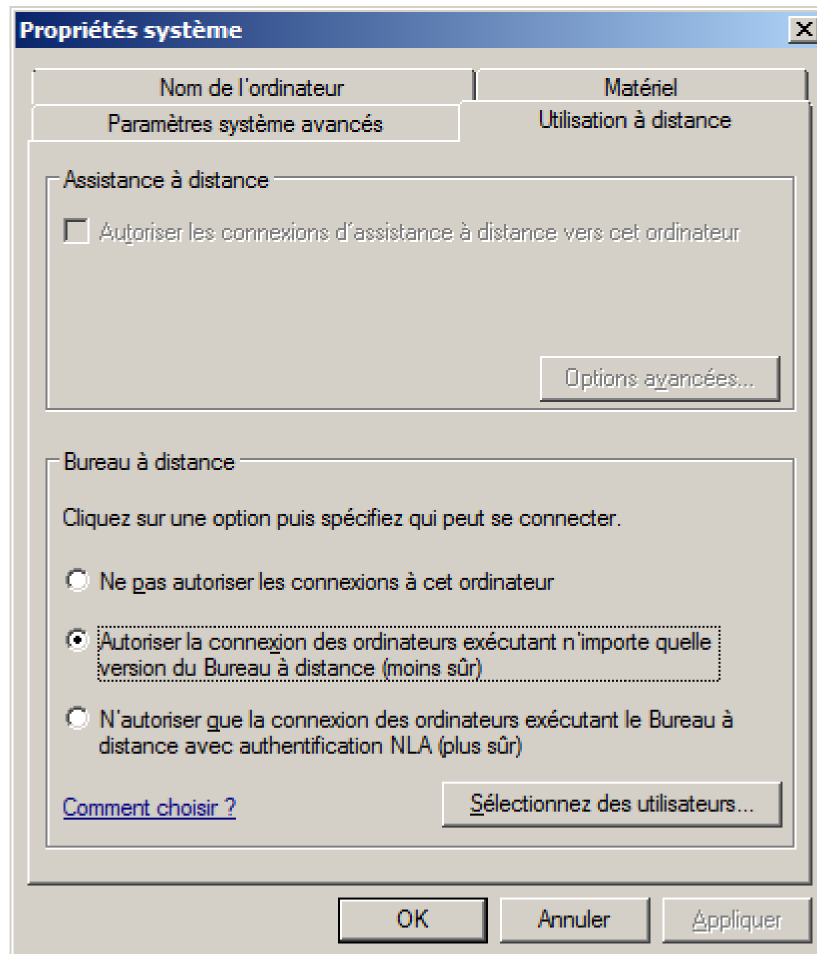


Figure 92 : Terminal Server : Compatibilité ascendante RDP

« **Sélectionnez des utilisateurs…** » fait apparaitre la fenêtre suivante :

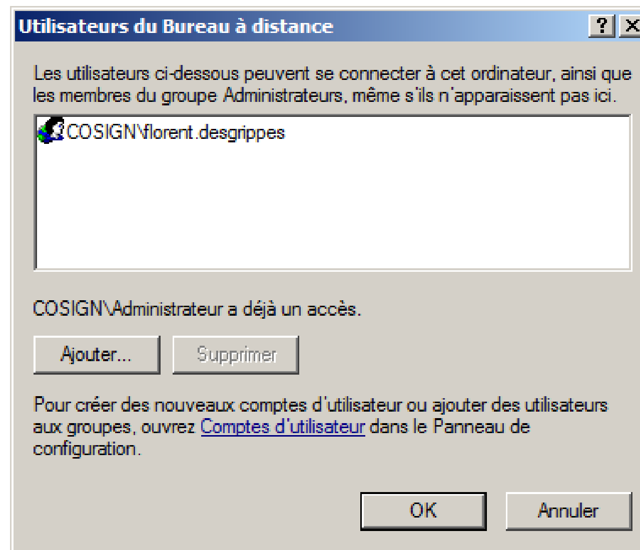


Figure 93 : Terminal Server : Ajout d'utilisateur du bureau à distance

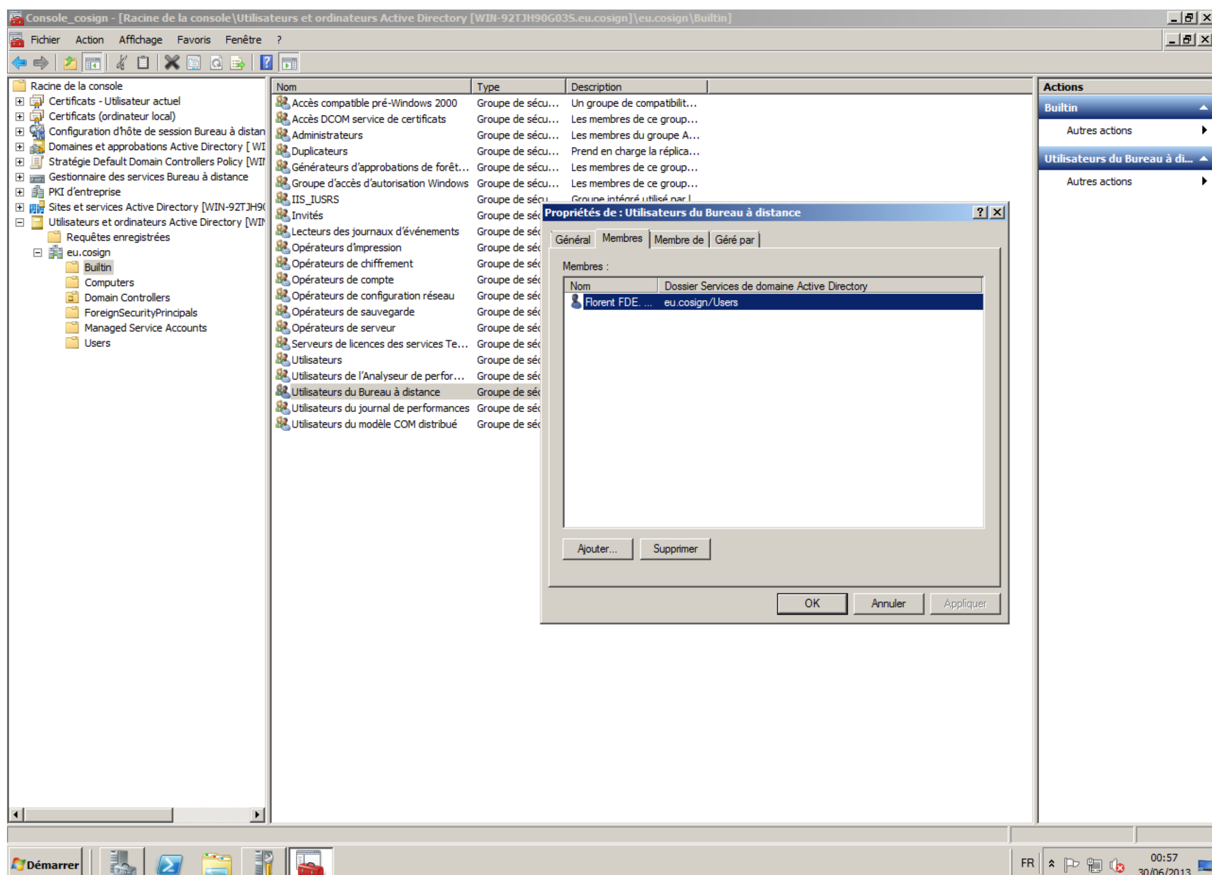


Figure 94 : Terminal Server : Groupe utilisateur du Bureau à distance

« **Démarrer > Exécuter…> secpol.msc** » :

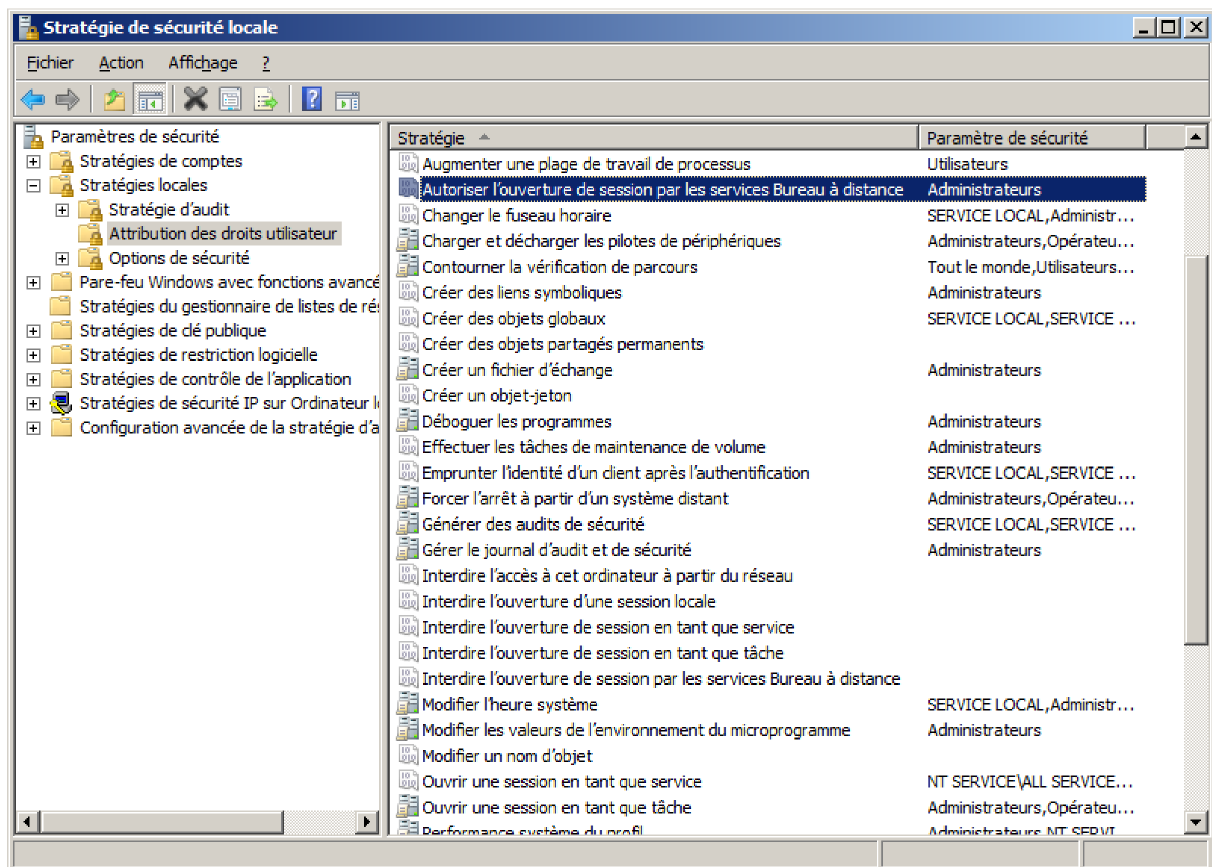


Figure 95 : Terminal Server : Droits d'ouverture de session à distance

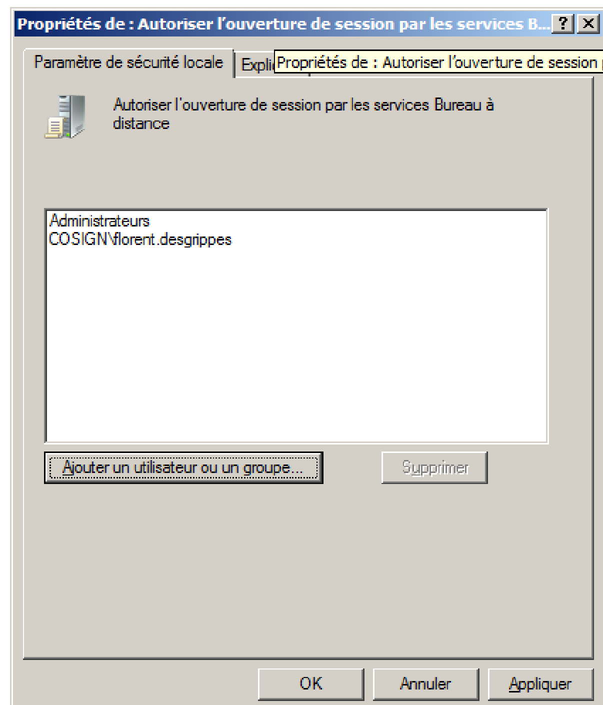


Figure 96 : Terminal Server : Droits d'ouverture de session à distance pour un utilisateur précis

Il est possible d'ajouter à cet endroit le groupe « **Utilisateur du Bureau à distance** » :

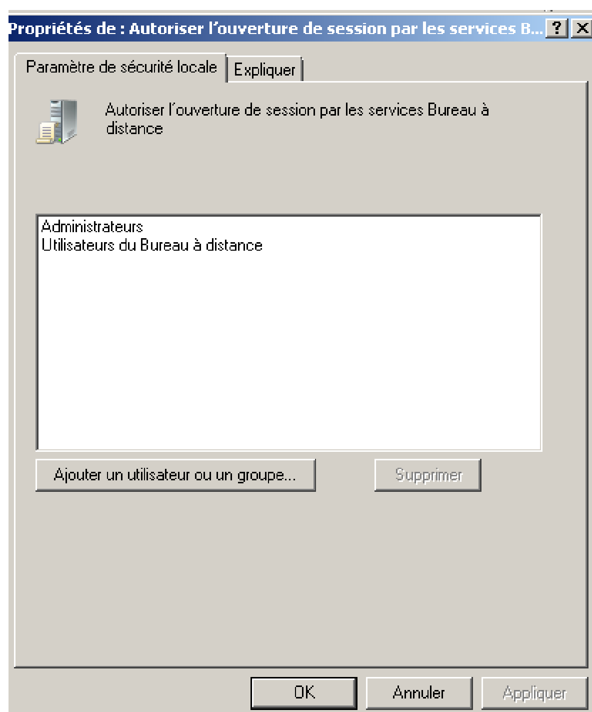


Figure 97 : Terminal Server : Droits d'ouverture de session à distance pour le groupe « Utilisateur du Bureau à distance »

12.6.7 Configuration du certificat du serveur RDP

Sur une infrastructure de production, le lien RDP doit être correctement paramétré.

En particulier, si le rôle AD CS est installé sur un serveur du SI, il est possible de faire signer le certificat serveur du lien RDP par l'autorité de certification racine de l'AD CS. De fait, ceci est même conseiller dans la mesure où le certificat racine de l'AD CS est provisionné via l'AD dans les magasins de certificats des postes clients.

http://blogs.msdn.com/b/rds/archive/2010/04/09/configuring-remote-desktop-certificates.aspx

(Malheureusement, documentation assez incomplète, un peu complétée ici) :

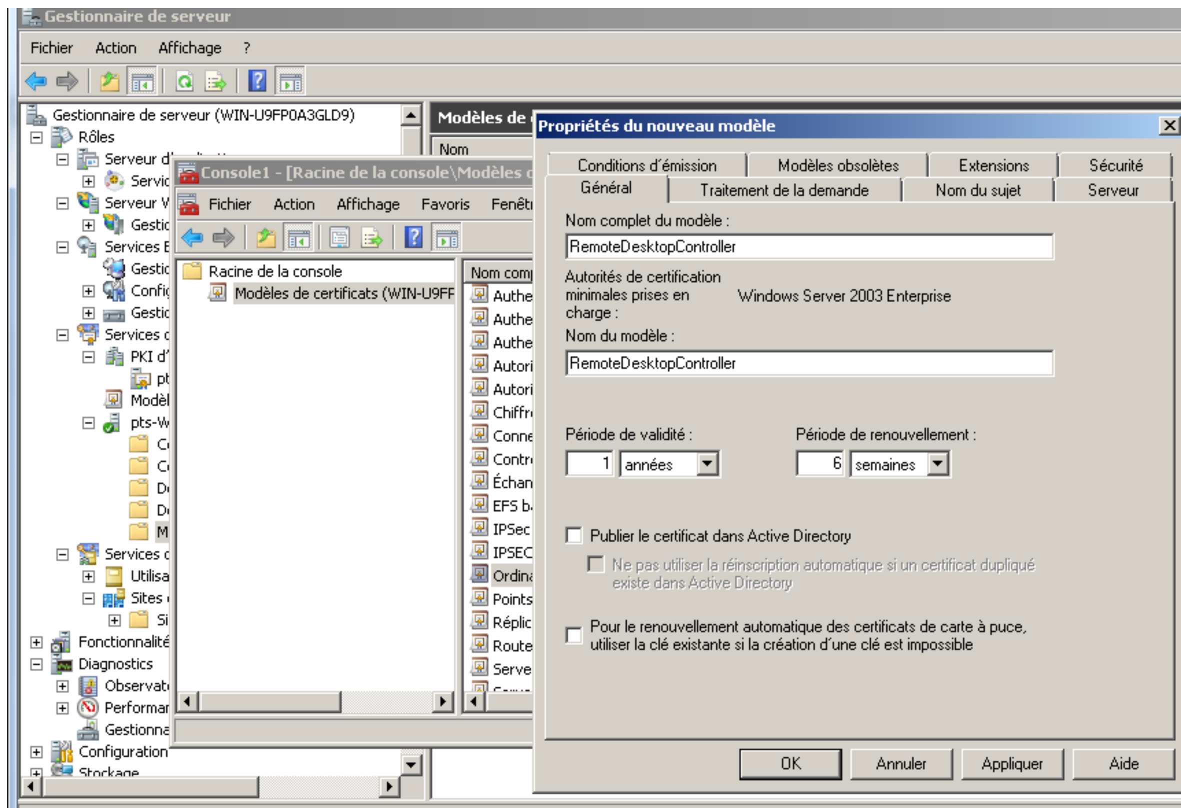


Figure 98 : Terminal Server : Création d'un modèle de certificat Remote Desktop sur l'AD CS

Propriétés de : RemoteDesktopComputer

Conditions d'émission | Modèles obsolètes | Extensions | Sécurité | Serveur
Général | Traitement de la demande | Nom du sujet

Nom complet du modèle :
RemoteDesktopComputer
Autorités de certification minimales prises en charge : Windows Server 2003 Enterprise
Nom du modèle :
RemoteDesktopComputer

Période de validité : 1 années
Période de renouvellement : 6 semaines

Publier le certificat dans Active Directory
Ne pas utiliser la réinscription automatique si un certificat dupliqué existe dans Active Directory
Pour le renouvellement automatique des certificats de carte à puce, utiliser la clé existante si la création d'une clé est impossible

OK | Annuler | Appliquer | Aide

Figure 99 : Terminal Server : Création d'un modèle de certificat Remote Desktop sur l'AD CS

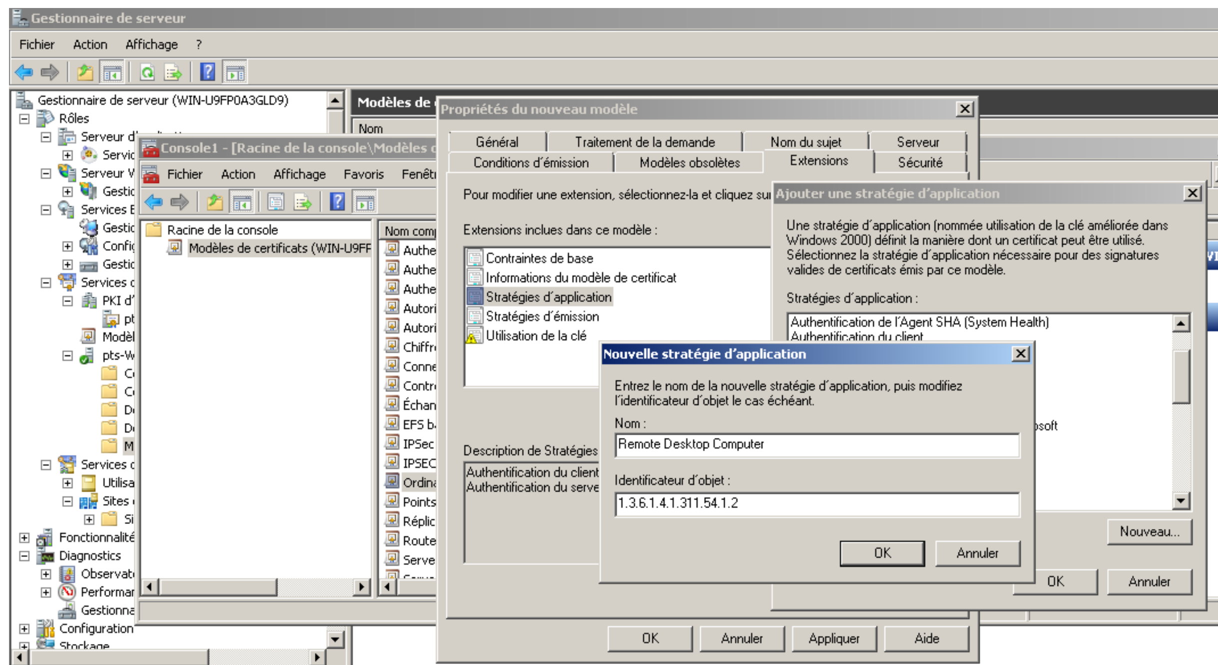


Figure 100 : Terminal Server : Création d'un modèle de certificat Remote Desktop sur l'AD CS

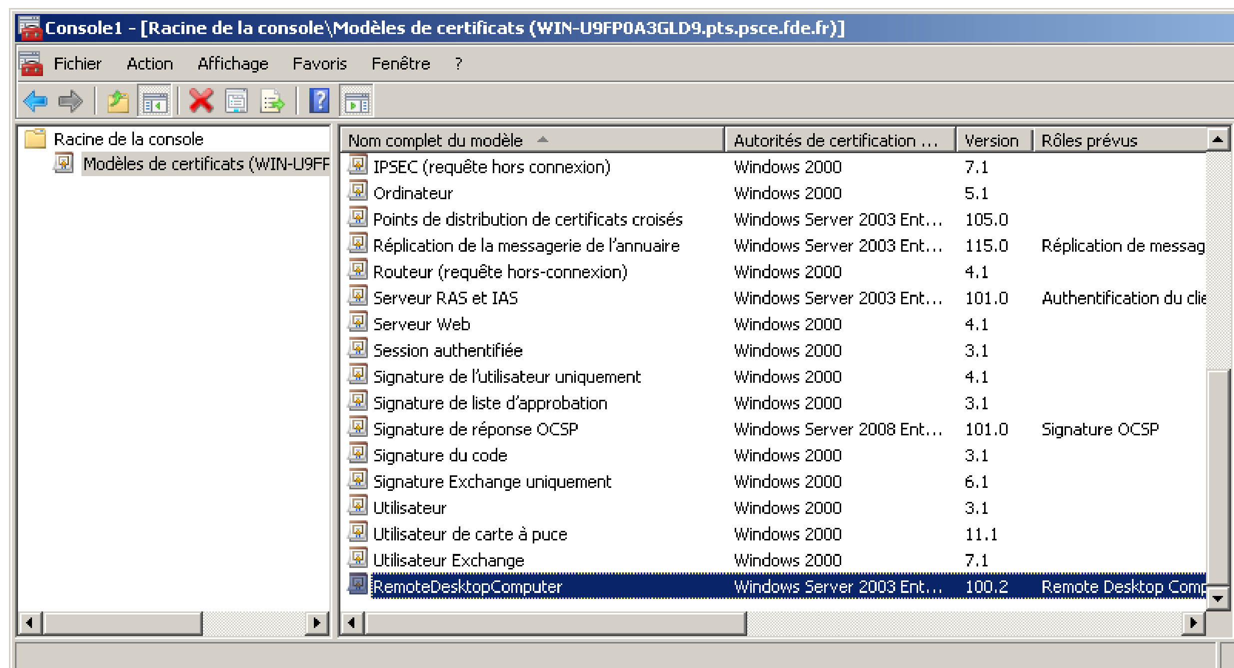


Figure 101 : Terminal Server : Création d'un modèle de certificat Remote Desktop sur l'AD CS

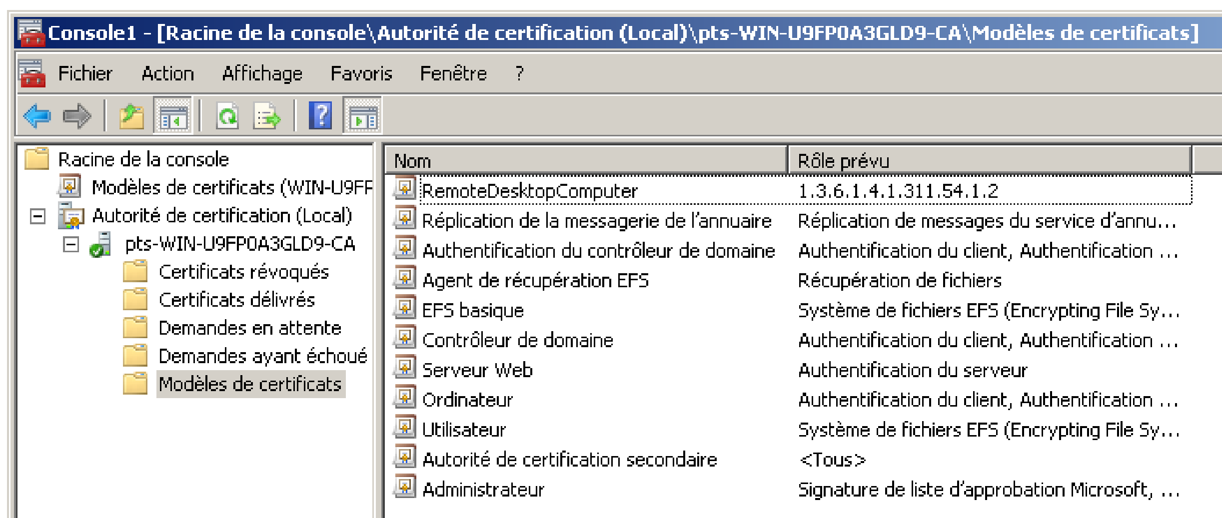


Figure 102 : Terminal Server : Création d'un modèle de certificat Remote Desktop sur l'AD CS

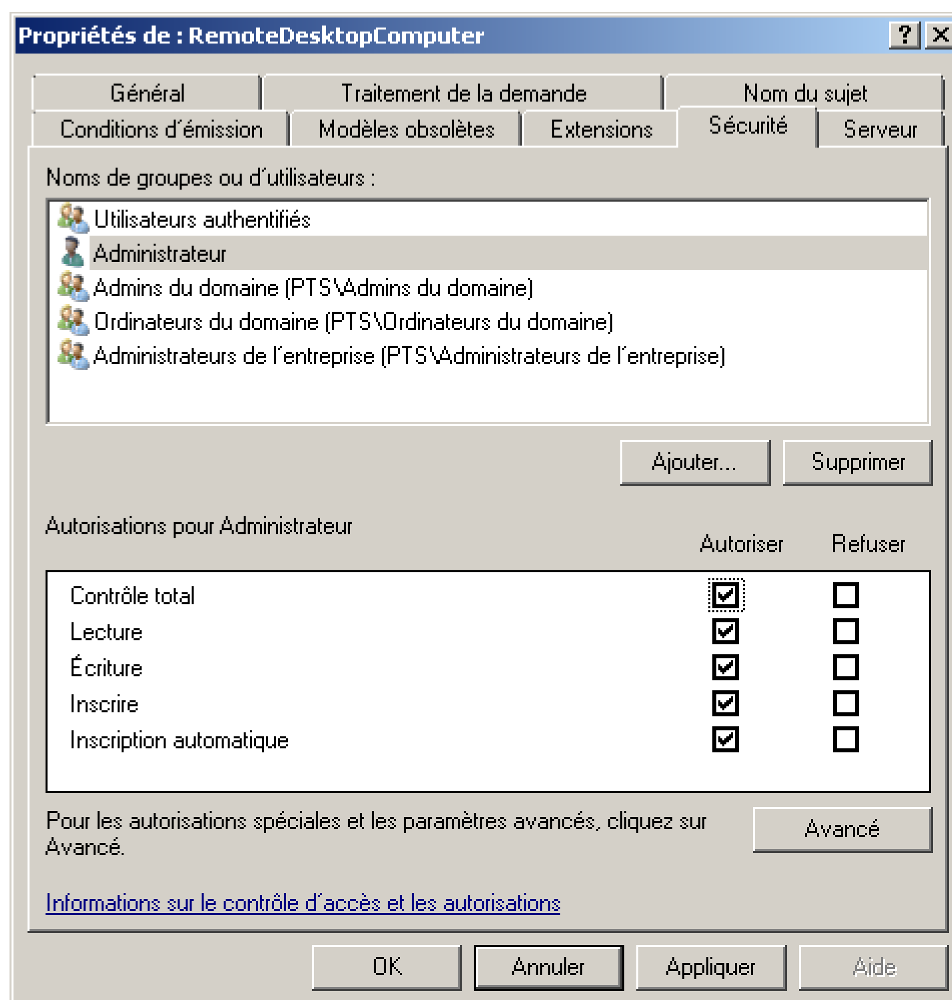


Figure 103 : Terminal Server : Droits sur le modèle de certificat Remote Desktop

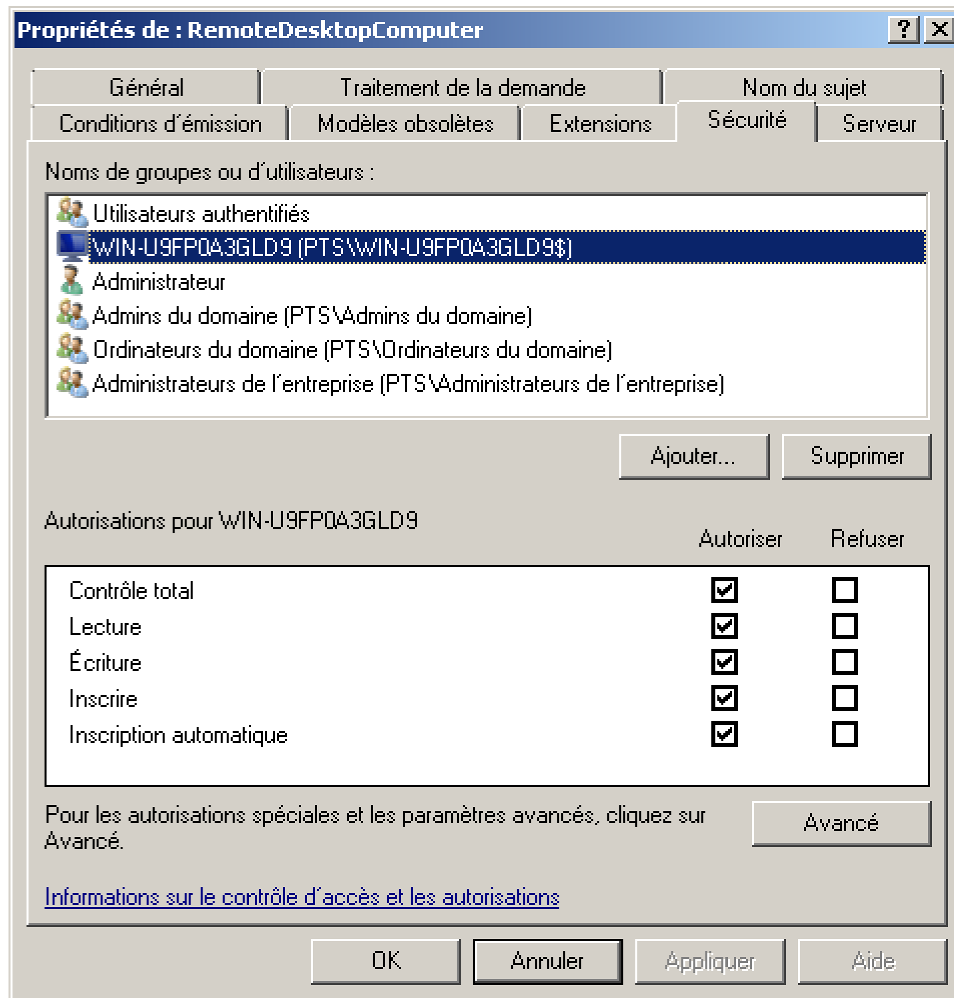


Figure 104 : Terminal Server : Droits sur le modèle de certificat Remote Desktop

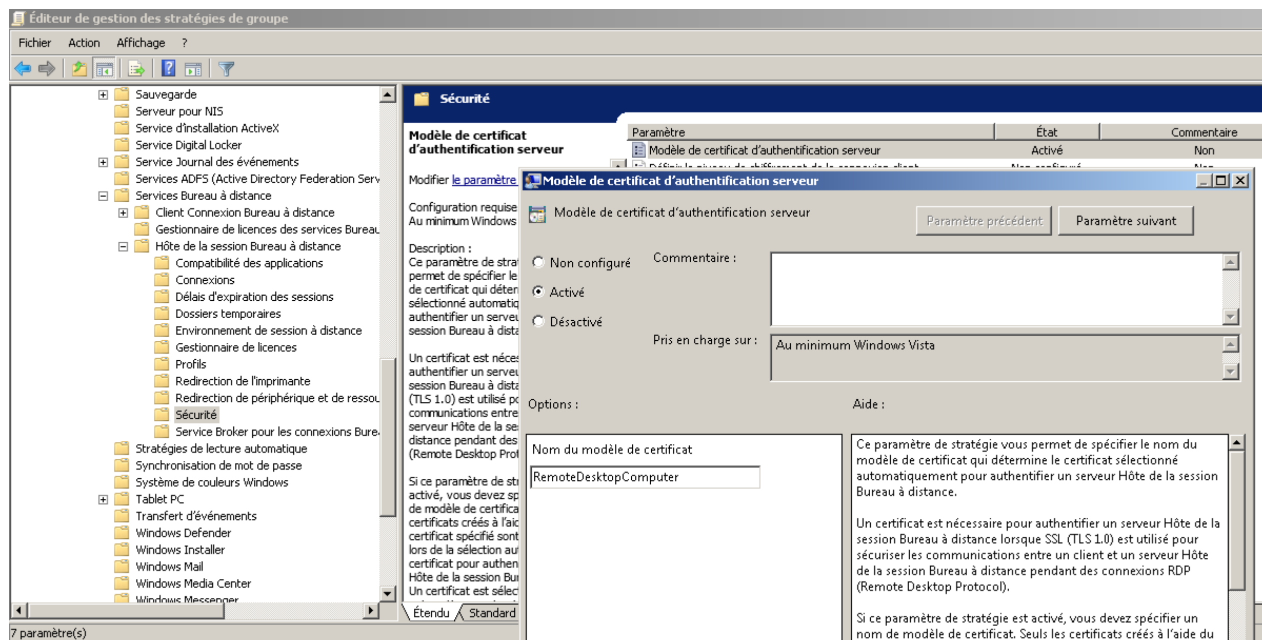


Figure 105 : Terminal Server : Déploiement du modèle de certificat Remote Desktop sur les postes clients via l'AD

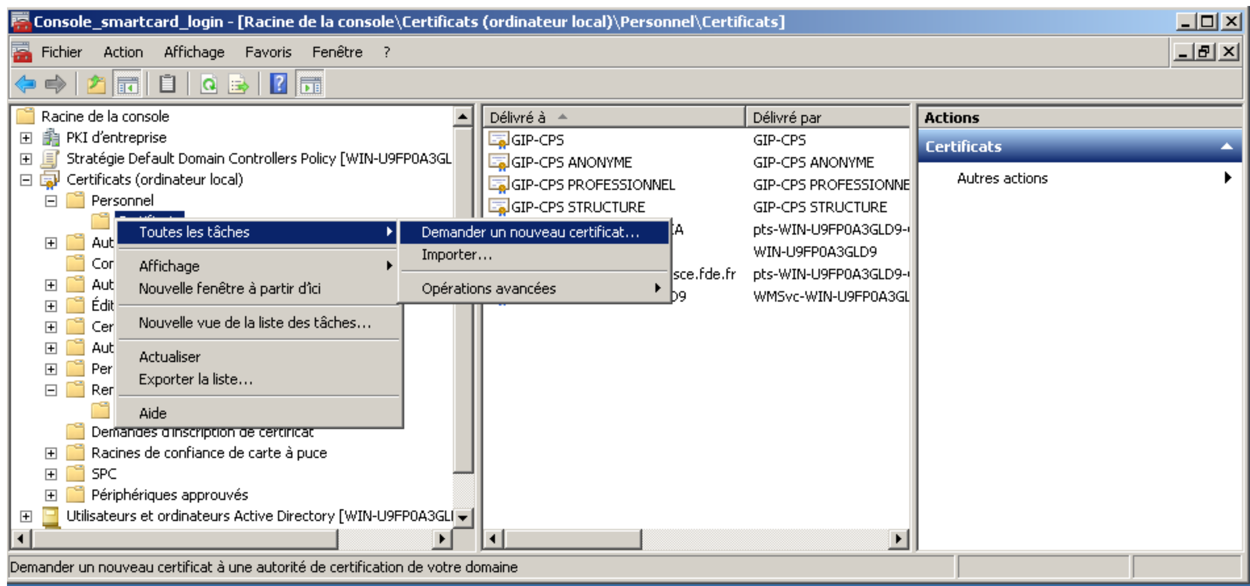


Figure 106 : Terminal Server : Demande de certificat Terminal Server

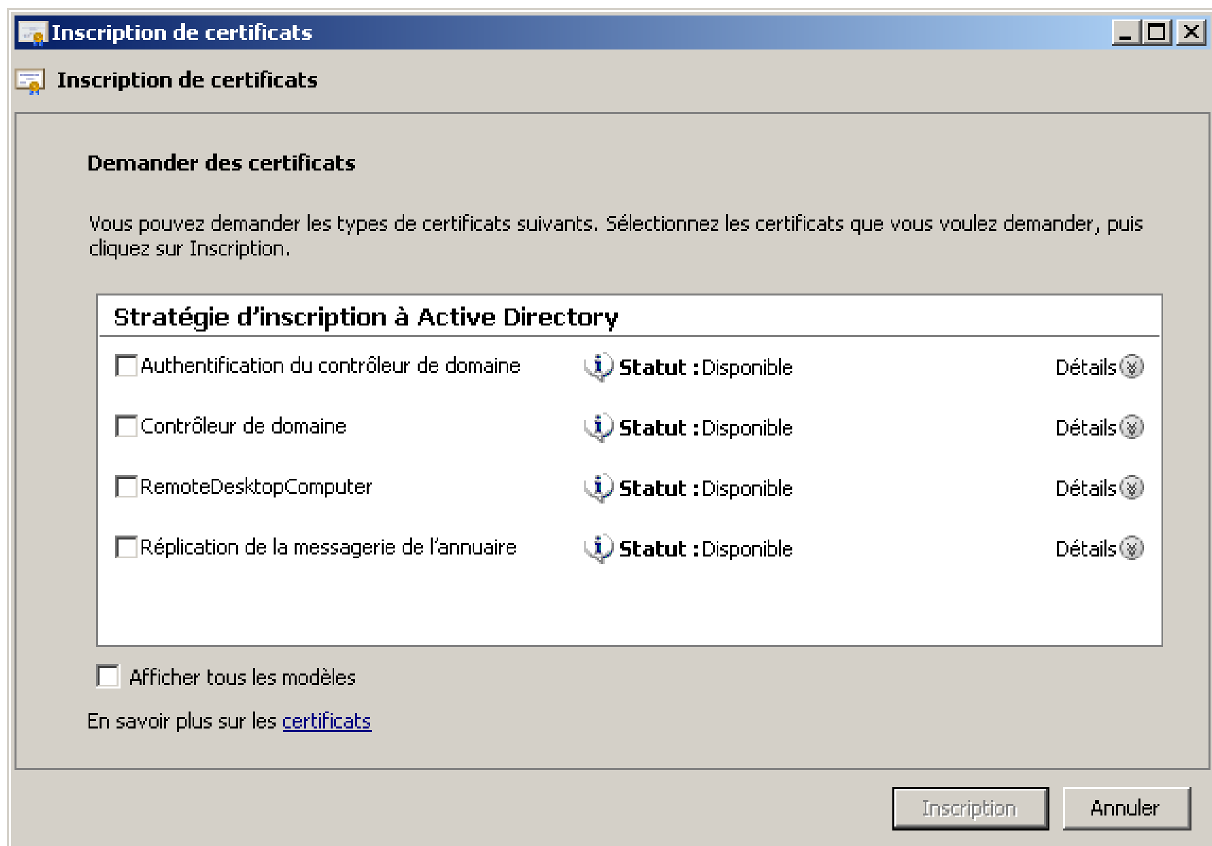


Figure 107 : Terminal Server : Demande de certificat Terminal Server : Sélection de « RemoteDesktopComputer »

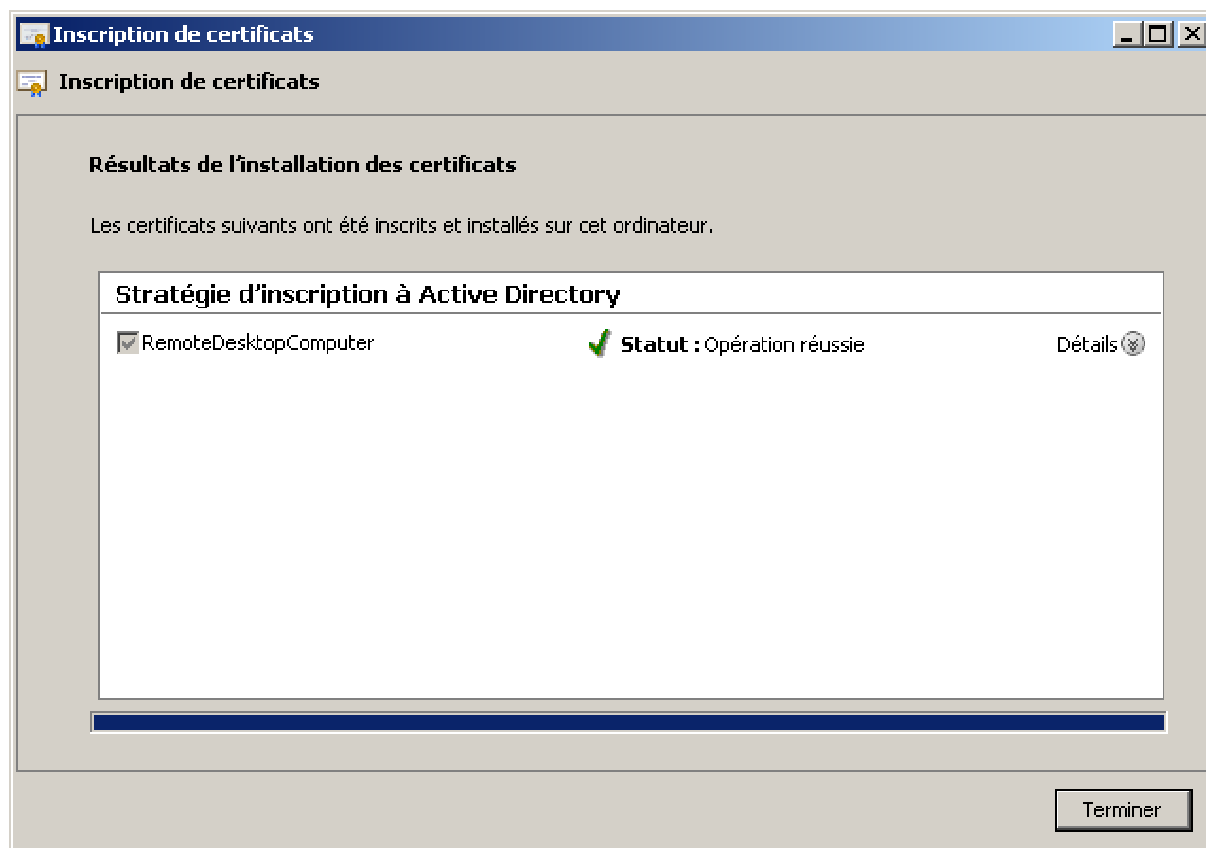


Figure 108 : Terminal Server : Demande de certificat Terminal Server

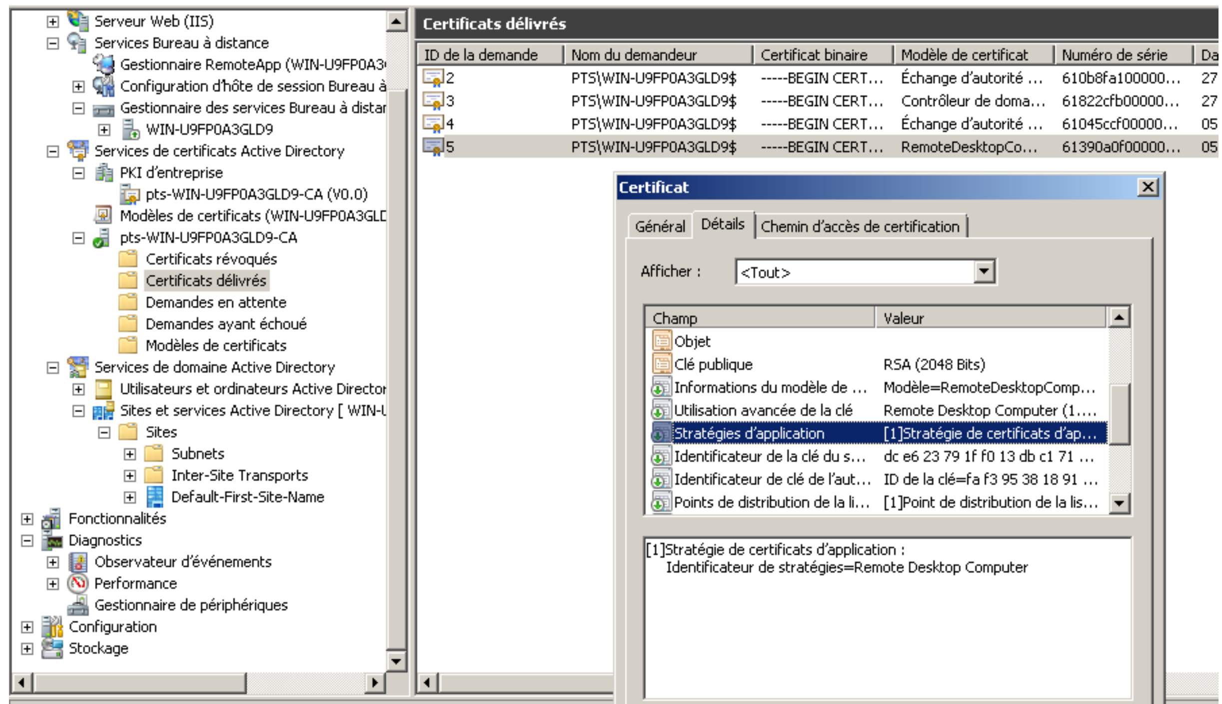


Figure 109 : Terminal Server : Vérification du certificat Terminal Server émis sur l'AD CS

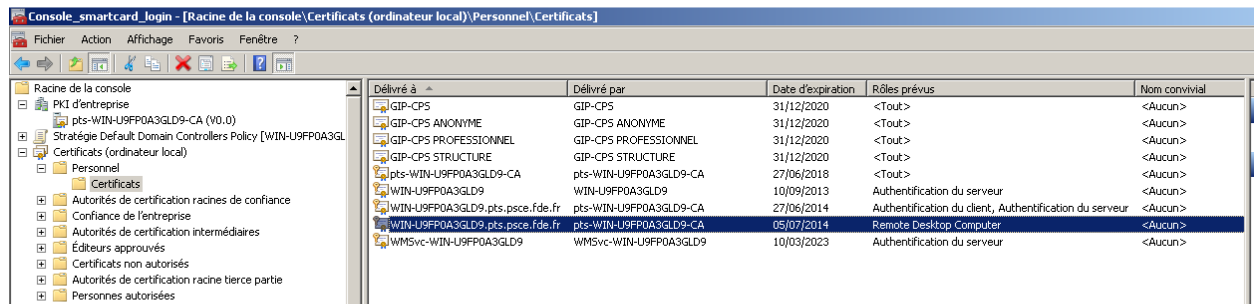


Figure 110 : Terminal Server : Vérification du certificat Terminal Server émis sur le Terminal Serveur

Conseil : sauvegarder ce certificat sous le nom %USERPROFILE%\Desktop**rd-rootca.cer**

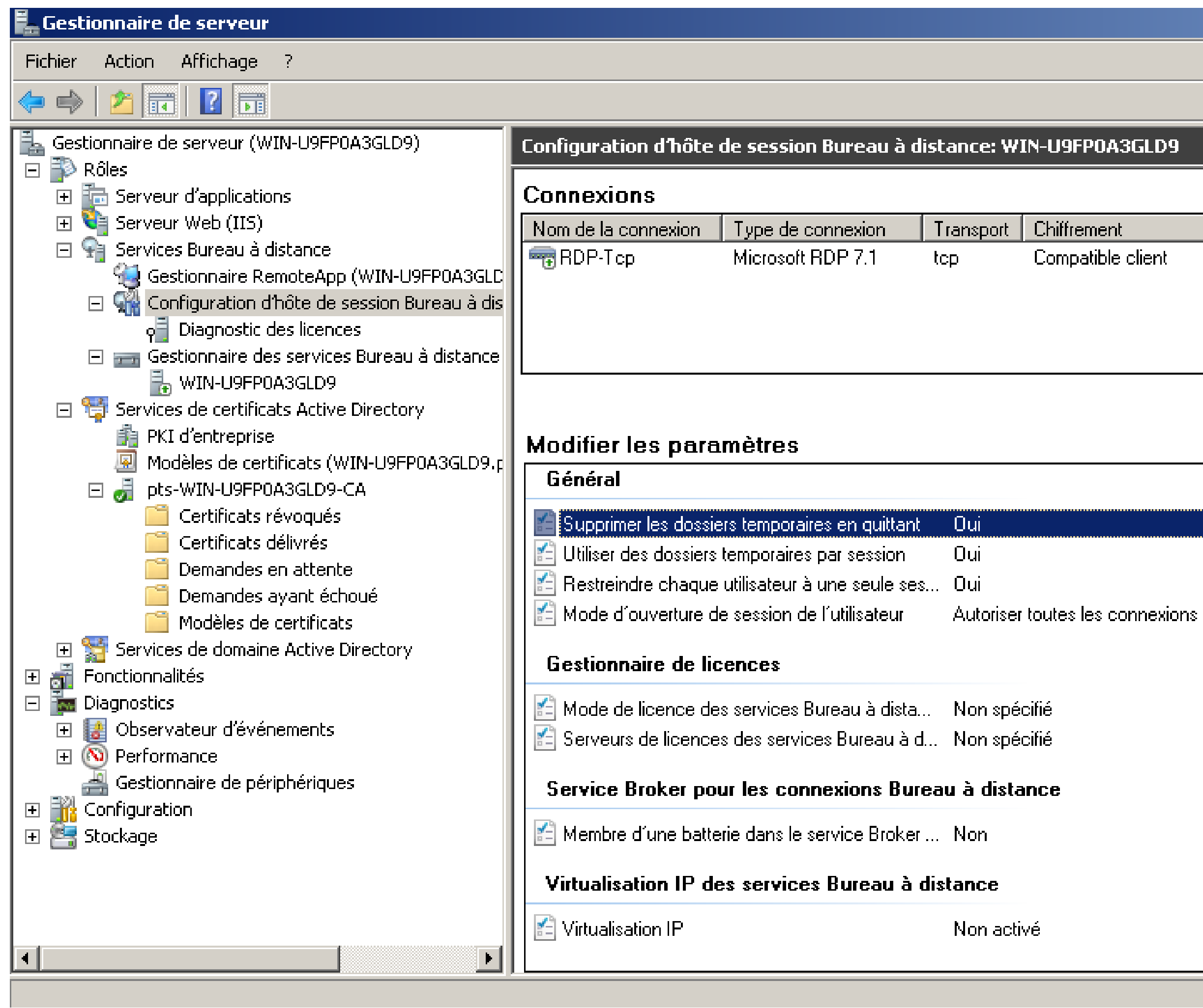


Figure 111 : Terminal Server : Installation du certificat Terminal Server

1. mmc.exe (Microsoft Management Console)
2. ajouter le composant enfichable: certificates (“computer” -> “ordinateur local” / “local computer”)
3. Répertoire “remote desktop” -> certificats
4. Effacer le certificate for the name of the server and close the mmc instance

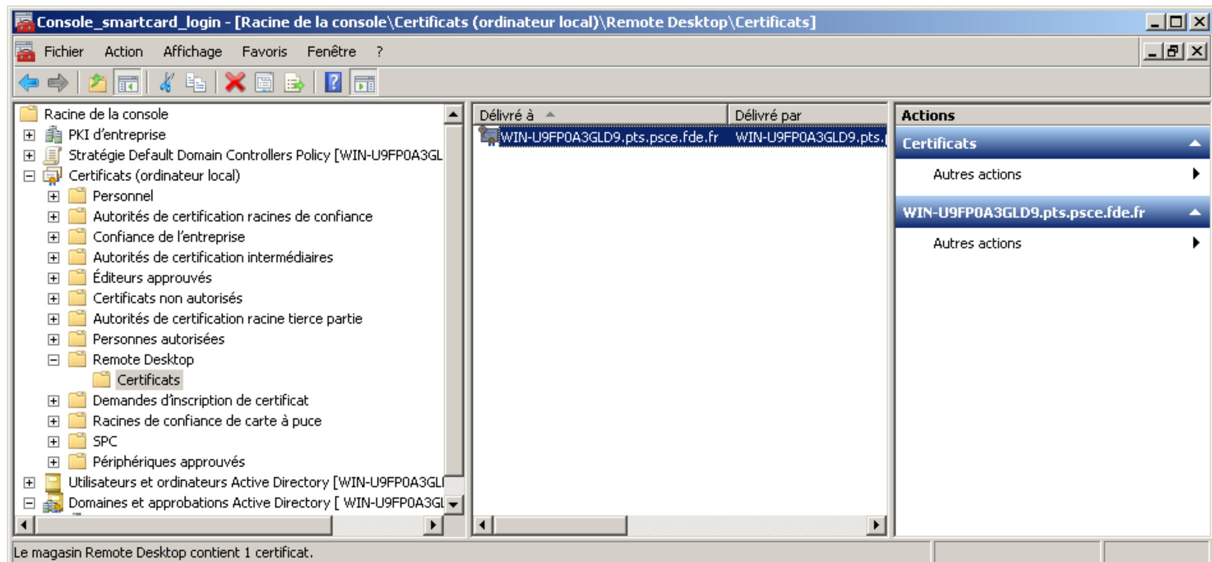


Figure 112 : Terminal Server : Configuration

5. Outils d’administration -> Services de bureau à distance -> Configuration d’hôte de session Bureau à distance
6. rdp -tcp -> clic droit -> propriétés

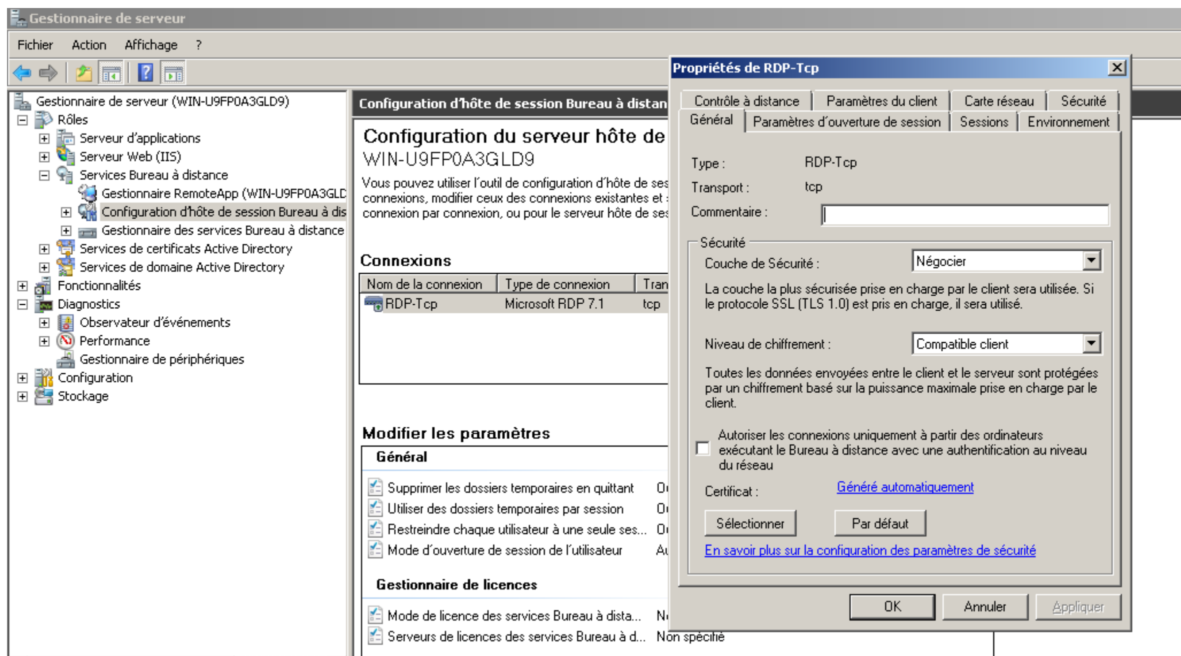


Figure 113 : Terminal Server : Installation du certificat Terminal Server

7. Sélectionner -> retrouver le certificat Remote Desktop :

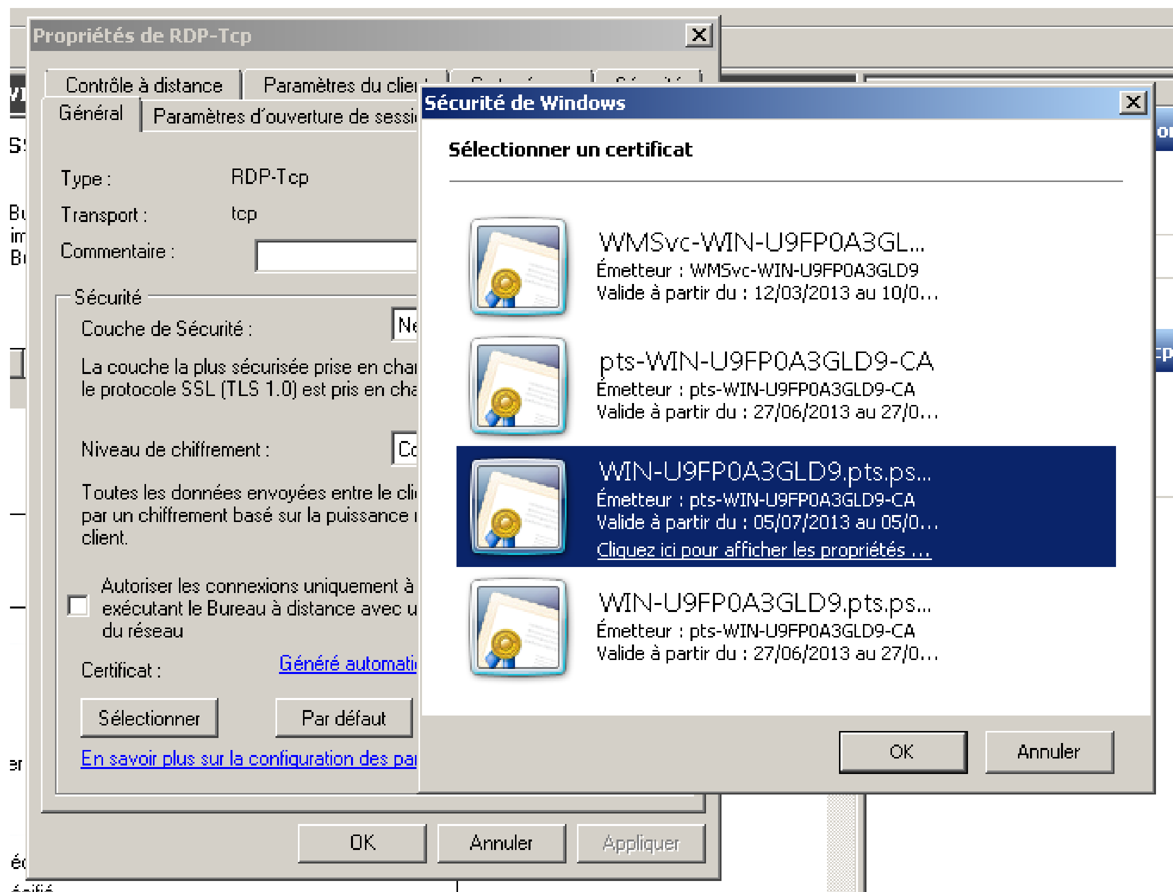


Figure 114 : Terminal Server : Installation du certificat Terminal Server

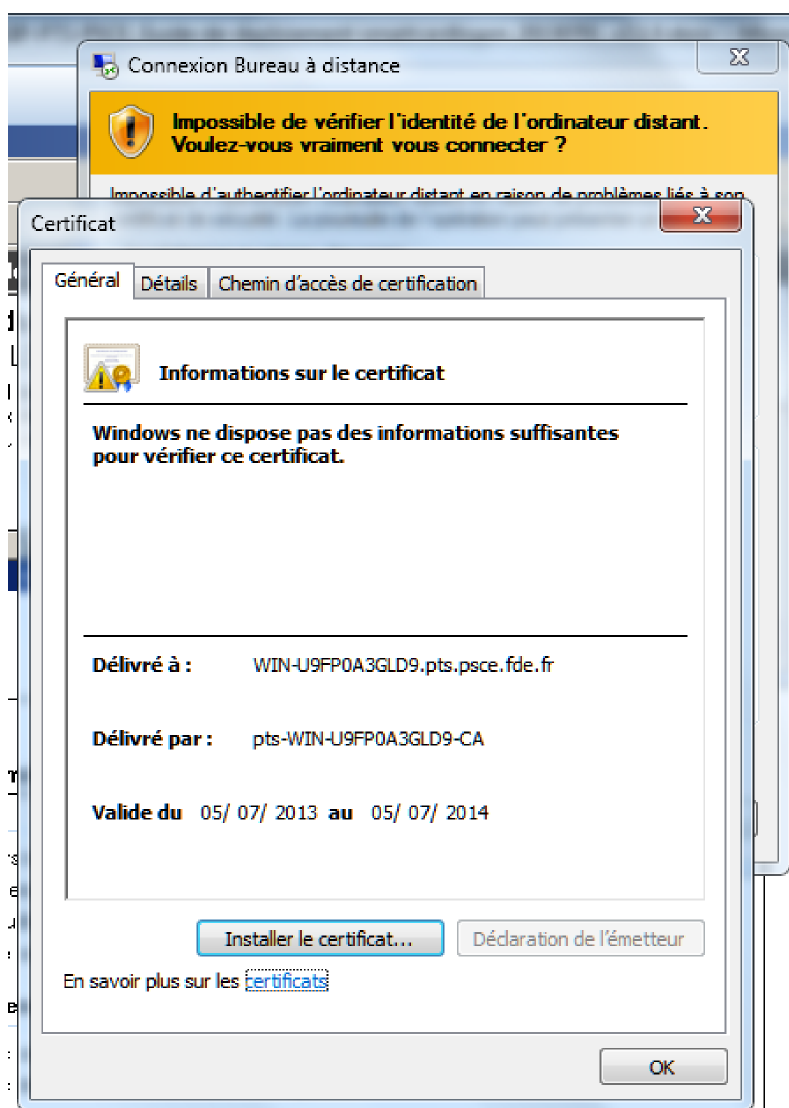


Figure 115 : Terminal Server : Vérifier l'installation du certificat Terminal Server

12.6.8 Autres GPOs

192.168.7.14 - Connexion Bureau à distance

Stratégie Default Domain Controllers Policy [FR-AS
Configuration ordinateur
Stratégies
Paramètres du logiciel
Installation de logiciel
Paramètres Windows
Stratégie de résolution de noms
Scripts (démarrage/arrêt)
Paramètres de sécurité
QoS basée sur la stratégie
Modèles d'administration : définitions d
Composants Windows
Analyse de fiabilité Windows
Assistance en ligne
Biométrie
Calendrier Windows
Carte à puce
Centre de mobilité Windows
Centre de sécurité
Chiffrement de lecteur BitLock
Compatibilité des applications
Emplacement et capteurs
Environnement distant Windov
Explorateur de jeux
Explorateur Windows
Flux RSS
Gadgets du Bureau
Gestion à distance de Window
Gestion des droits numériques
Gestionnaire de fenêtres du B
Gestionnaire de ressources sy
Groupe résidentiel
Interface utilisateur d'informat
Internet Explorer
Internet Information Services
Lecteur Windows Media
Magnétophone
Mise à niveau express
NetMeeting
Observateur d'événements
Options d'arrêt
Options d'ouverture de sessio
Paramètres de présentation
Parental Controls
Planificateur de tâches
Programme d'amélioration de l
Projecteur réseau
Protection d'accès réseau
Rapport d'erreurs Windows
Sauvegarde
Serveur pour NIS

Connexions

N'autoriser qu'une session de services Bureau à distance par utilisateur

Modifier le paramètre de stratégie

Configuration requise :
Au minimum Windows Server 2003

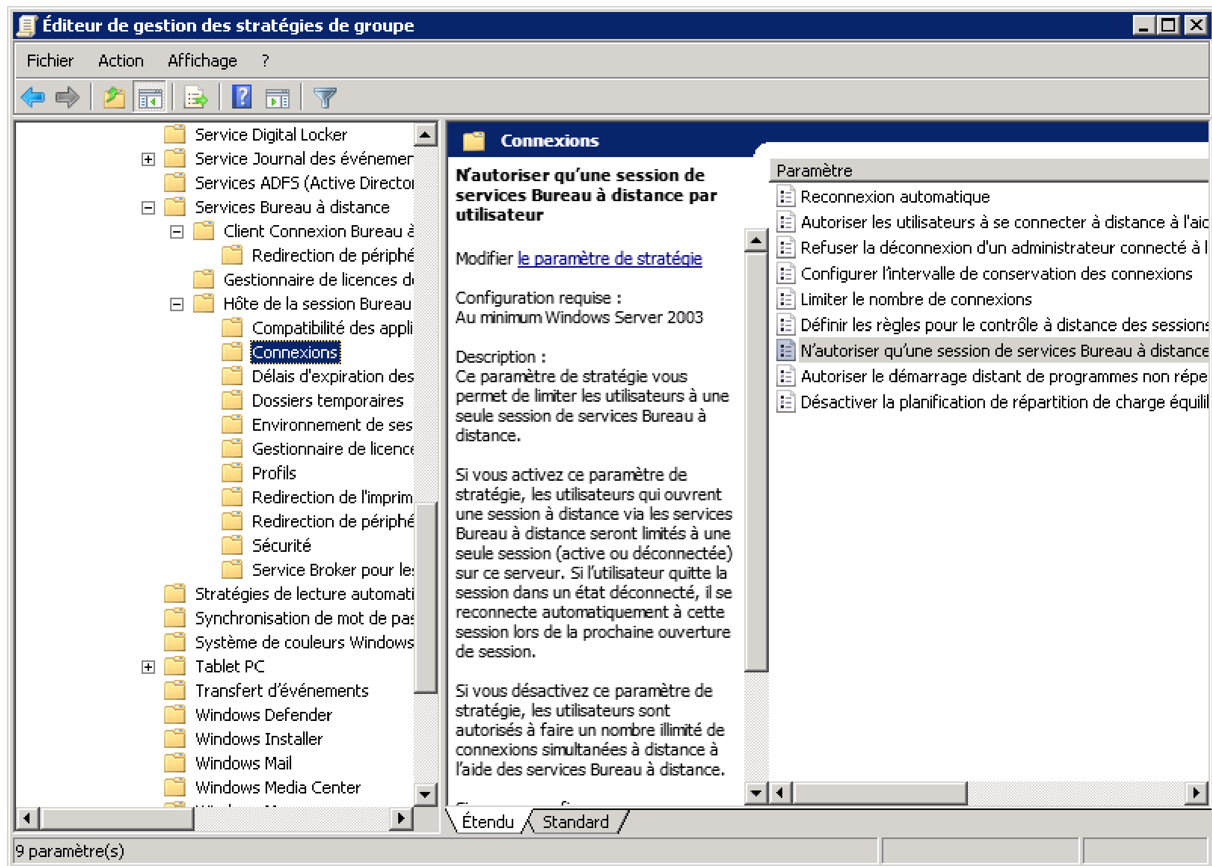
Description :
Ce paramètre de stratégie vous permet de limiter les utilisateurs à une seule session de services Bureau à distance.

Si vous activez ce paramètre de stratégie, les utilisateurs qui ouvrent une session à distance via les services Bureau à distance seront limités à une seule session (active ou déconnectée) sur ce serveur. Si l'utilisateur quitte la session dans un état déconnecté, il se reconnecte automatiquement à cette session lors de la prochaine ouverture de session.

Si vous désactivez ce paramètre de stratégie, les utilisateurs sont autorisés à faire un nombre illimité de connexions simultanées à distance à l'aide des services Bureau à distance.

Si vous ne configurez pas ce paramètre de stratégie, le paramètre « Limiter les utilisateurs à une seule session » de l'outil Configuration de l'hôte de la session Bureau à distance détermine si les utilisateurs sont limités à une seule session de services Bureau à distance.

Paramètre	État
Reconnexion automatique	Non configuré
Autoriser les utilisateurs à se connecter à distance à l'aide des se…	Non configuré
Refuser la déconnexion d'un administrateur connecté à la session…	Non configuré
Configurer l'intervalle de conservation des connexions	Non configuré
Limiter le nombre de connexions	Non configuré
Définir les règles pour le contrôle à distance des sessions utilisate…	Non configuré
N'autoriser qu'une session de services Bureau à distance par utilis…	Désactivé
Autoriser le démarrage distant de programmes non répertoriés	Non configuré
Désactiver la planification de répartition de charge équilibrée du t…	Non configuré


Éditeur de gestion des stratégies de groupe
Fichier Action Affichage ?
Service Digital Locker
Service Journal des événemer
Services ADFS (Active Directo
Services Bureau à distance
Client Connexion Bureau à
Redirection de périphé
Gestionnaire de licences d
Hôte de la session Bureau
Compatibilité des appli
Connexions
Délais d'expiration des
Dossiers temporaires
Environnement de ses
Gestionnaire de licence
Profils
Redirection de l'imprim
Redirection de périphé
Sécurité
Service Broker pour le
Stratégies de lecture automati
Synchronisation de mot de pas
Système de couleurs Windows
Tablet PC
Transfert d'événements
Windows Defender
Windows Installer
Windows Mail
Windows Media Center
Connexions
N'autoriser qu'une session de services Bureau à distance par utilisateur
Modifier le paramètre de stratégie
Configuration requise :
Au minimum Windows Server 2003
Description :
Ce paramètre de stratégie vous permet de limiter les utilisateurs à une seule session de services Bureau à distance.
Si vous activez ce paramètre de stratégie, les utilisateurs qui ouvrent une session à distance via les services Bureau à distance seront limités à une seule session (active ou déconnectée) sur ce serveur. Si l'utilisateur quitte la session dans un état déconnecté, il se reconnecte automatiquement à cette session lors de la prochaine ouverture de session.
Si vous désactivez ce paramètre de stratégie, les utilisateurs sont autorisés à faire un nombre illimité de connexions simultanées à distance à l'aide des services Bureau à distance.
Paramètre
Reconnexion automatique
Autoriser les utilisateurs à se connecter à distance à l'aic
Refuser la déconnexion d'un administrateur connecté à l
Configurer l'intervalle de conservation des connexions
Limiter le nombre de connexions
Définir les règles pour le contrôle à distance des sessions
N'autoriser qu'une session de services Bureau à distance
Autoriser le démarrage distant de programmes non répe
Désactiver la planification de répartition de charge équili
Étendu
Standard
9 paramètre(s)

12.7 Installation d'un rôle IIS

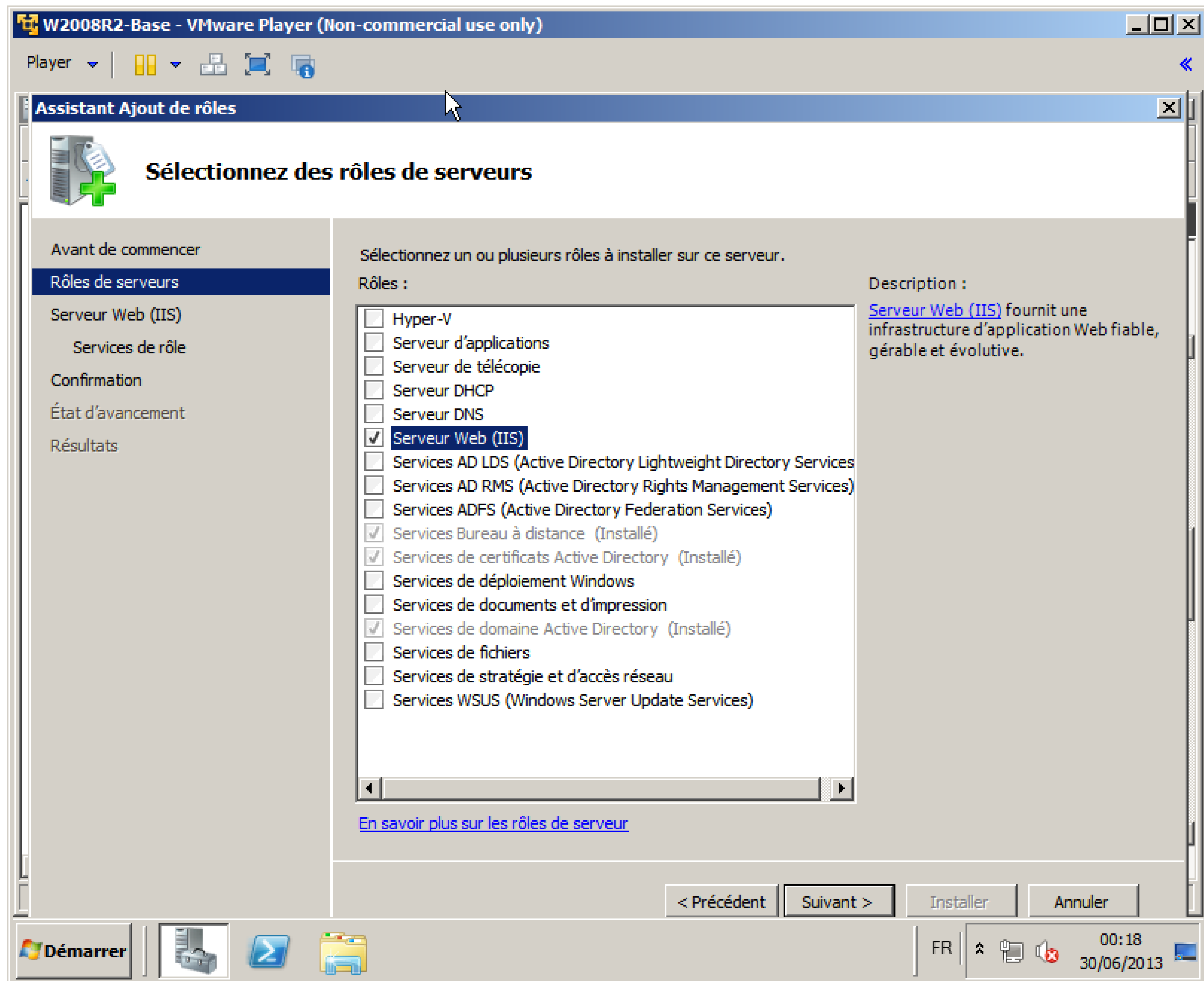


Figure 116 : IIS: Installation du rôle

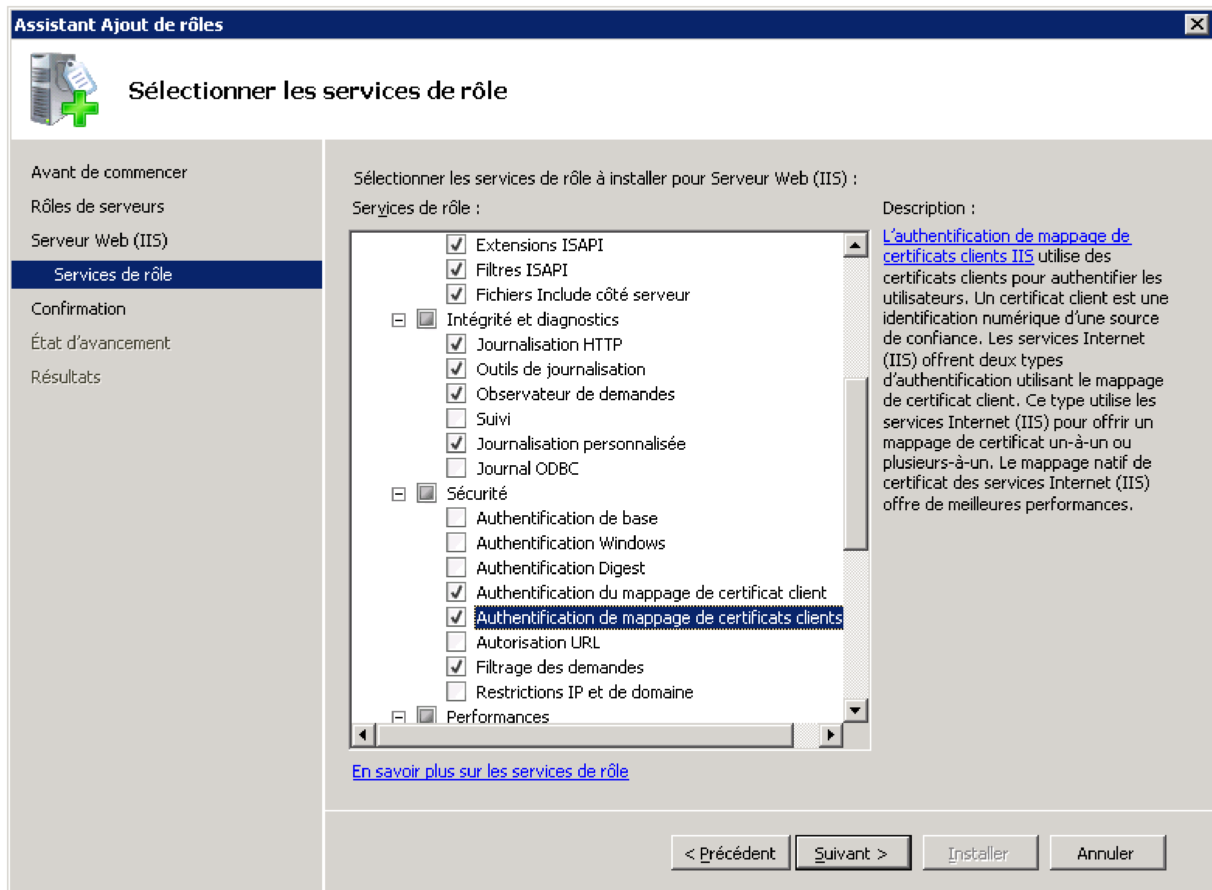


Figure 117 : IIS: Installation du rôle : sélection des options de sécurité

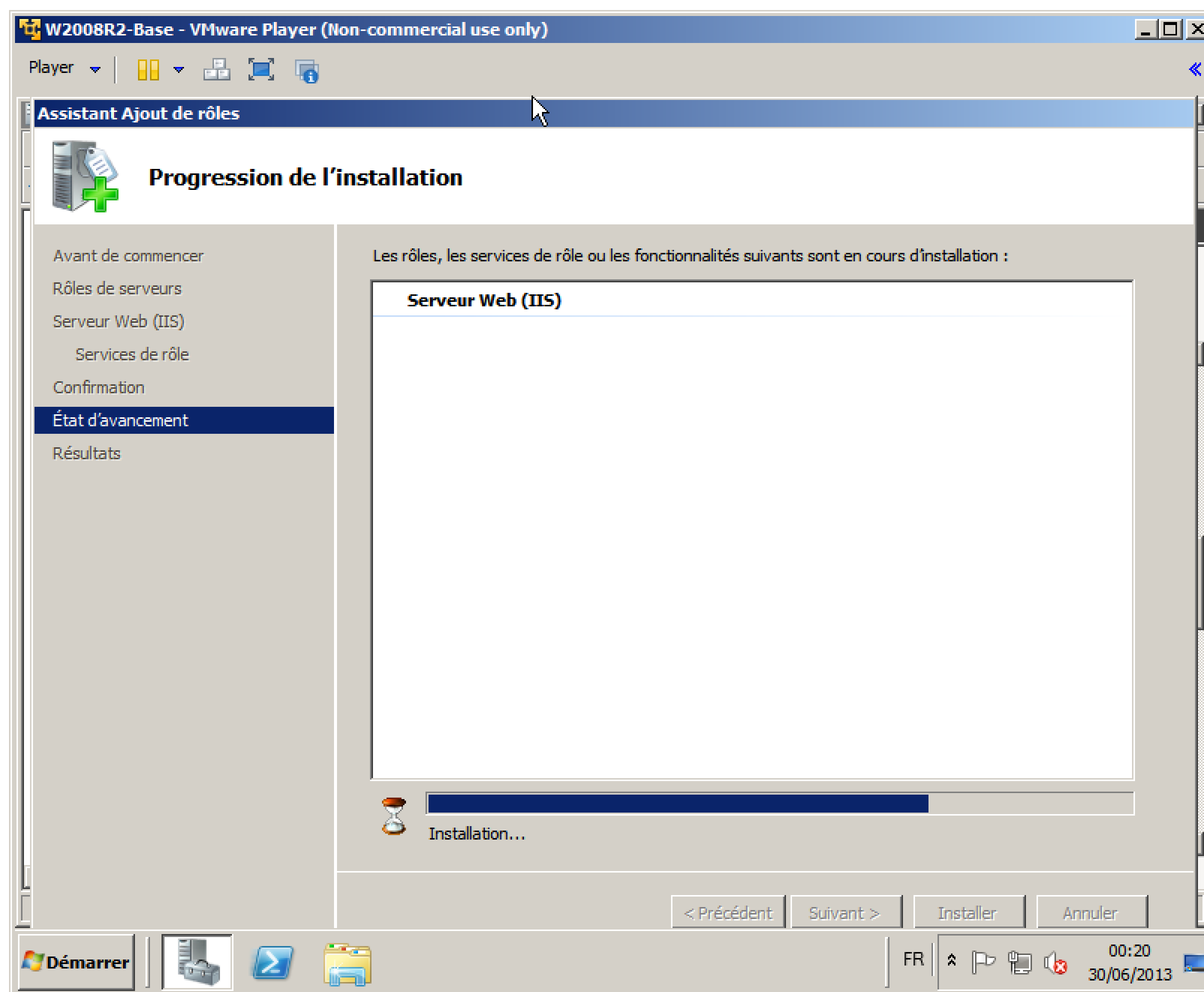


Figure 118 : IIS: Installation du rôle : état d'avancement

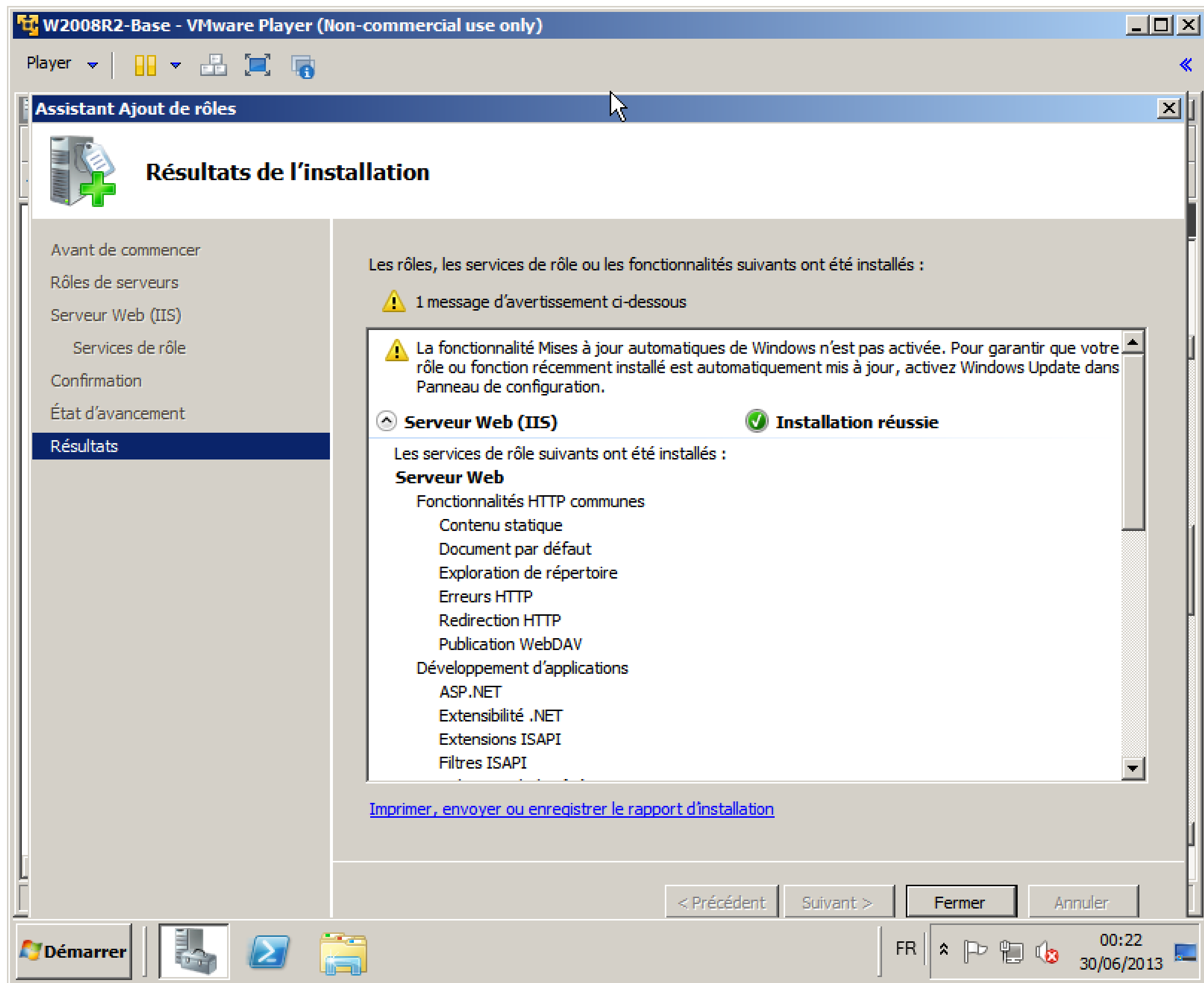


Figure 119 : IIS: Installation du rôle : Résultat

12.8 Installation de la Cryptolib CPS sur le serveur

Afin de pouvoir faire du Smartcard logon à base de CPS via TSE, il est nécessaire d'installer les Cryptolib CPS 64bit sur le serveur TSE en étant administrateur de la machine, en sus du rôle « Terminal Server ». cf. « Points d'attention » par ailleurs.

Conseil : ne pas laisser les fichiers .msi d'installation sur un serveur de production (sécurité), à défaut : vérifier que les droits accordés sur les .msi sont adéquates.

12.8.1 Désactivation du CCM au lancement

Dans ce cas, sur le serveur, il est conseillé de ne pas lancer le CCM automatiquement :

démarrer > **exécuter**…> « **msconfig** » > « **Démarrage** » > **décocher « CPS CCM »** (reboot requis mais une option « ultérieurement » permet d'attendre le prochain reboot).

12.8.2 Activation du CCM à l'ouverture de session au cas par cas

Eventuellement, lancer le CCM au démarrage des sessions utilisateurs (copie du raccourci « CCM.exe » dans le répertoire « Démarrage » du profil de l'utilisateur - %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup):

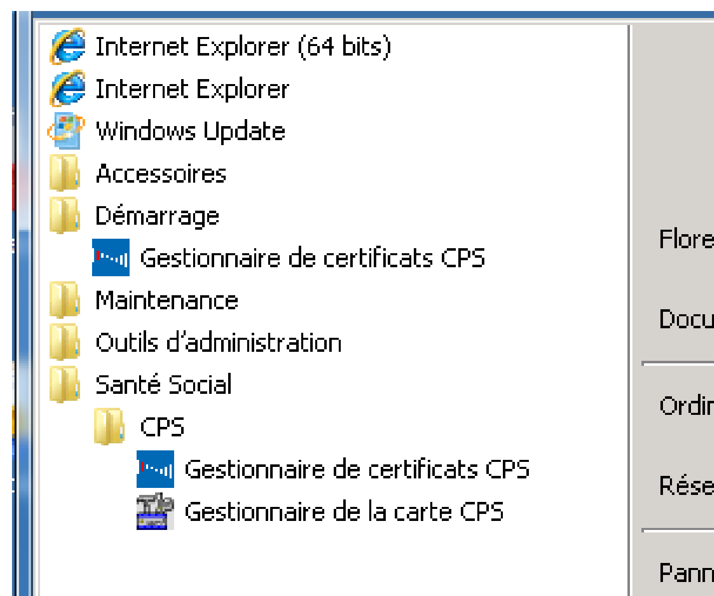


Figure 120 : CCM: lancement du CCM au démarrage des sessions utilisateurs sur un serveur Windows

12.8.3 Remarque sur le provisionning des magasins de certificats

Si l'installation de la Cryptolib CPS est réalisée côté serveur, les magasins de certificats (root et intermédiaire) sont provisionnés avec les certificats ASIP Santé de production.
Si des cartes de test sont utilisées en maquette, il faut tout de même provisionner ces magasins avec les chaines de tests (voir Configuration du Contrôleur de domaine pour la Smartcard logon).

12.9 Installation du Provider de révocation ASIP Santé – Microsoft sur le serveur

Le Provider de révocation ASIP Santé développé par Microsoft doit être installé sur chaque contrôleur de domaine pour la vérification des CRLs des certificats client de la carte.

12.9.1 Installation du Provider de révocation ASIP Santé – Microsoft

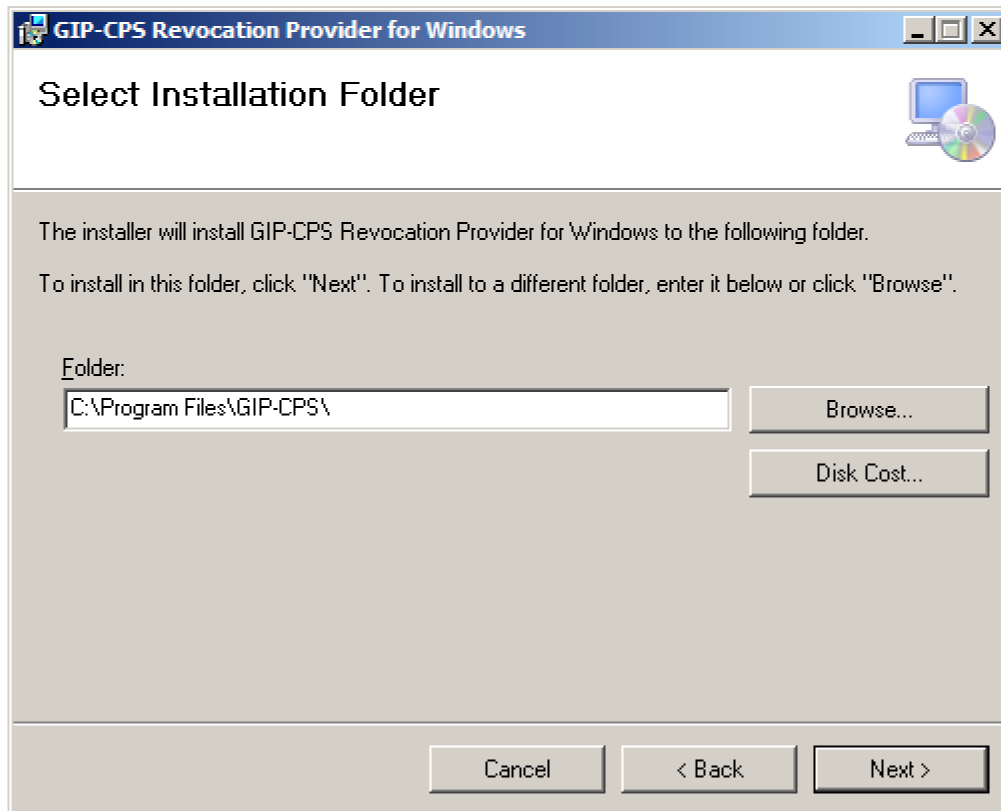


Figure 121 : CPSRev: répertoire d'installation

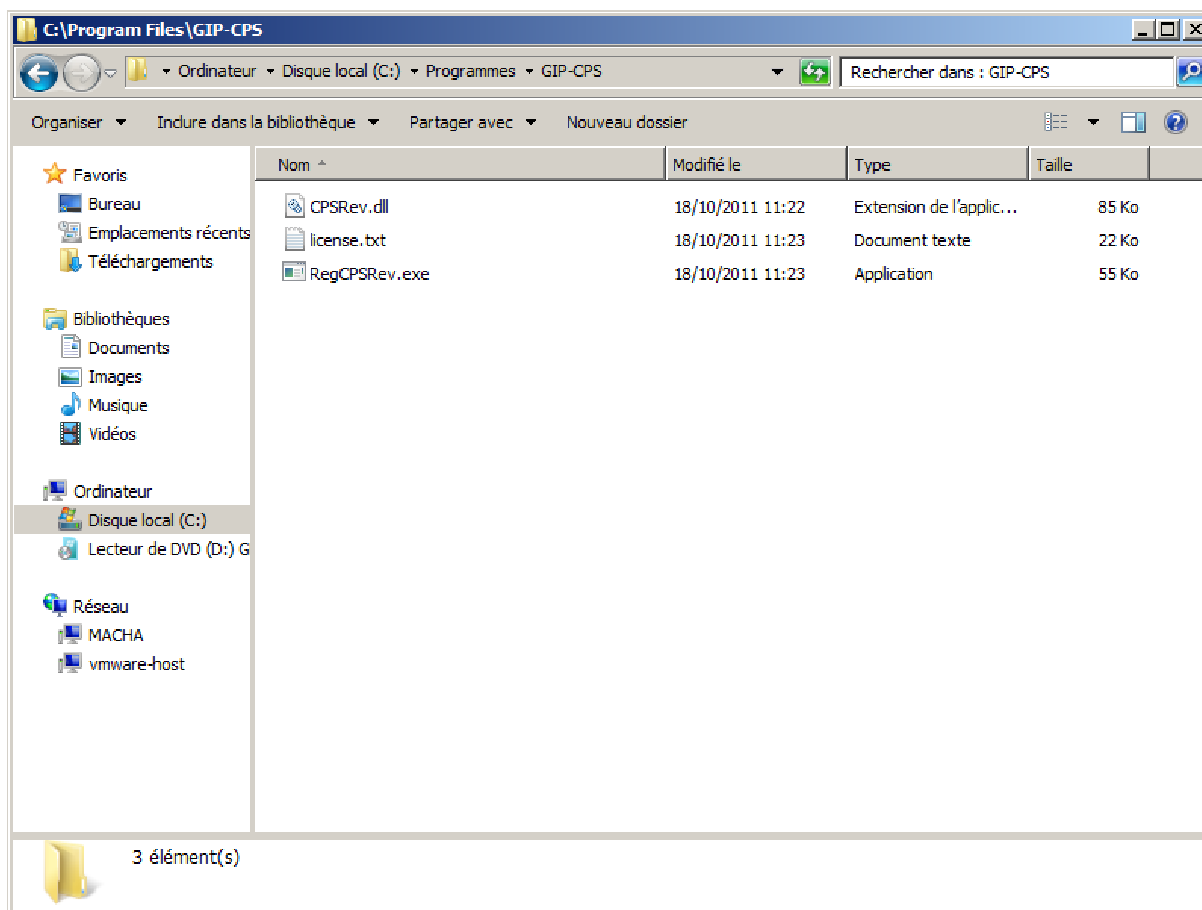


Figure 122 : CPSRev: résultat d'installation

12.9.2 Mise à jour des magasins de certificats Local Machine

Il est ensuite nécessaire de mettre à jour les magasins de certificats Local machine.

Vérifier le magasin « Local machine \ racine » : Les certificats ASIP Santé racine doivent être présents.

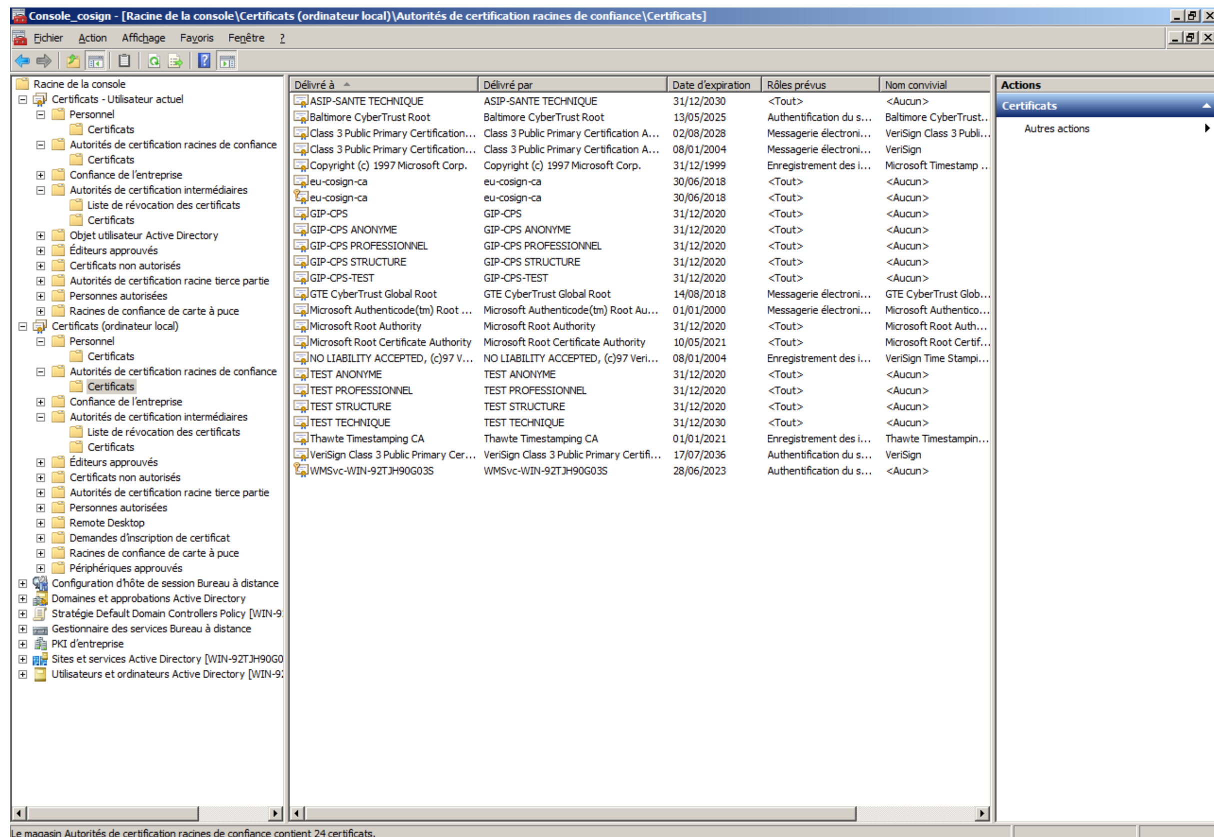


Figure 123 : CPSRev: vérification du magasin Root (Local machine)

A minima, les 5 certificats racine de production de l'ASIP Santé doivent être présents (se reporter au chapitre « Détails de certificat »):

Si des cartes de test sont utilisées (environnements de tests et d'homologation), les 5 certificats racine de test de l'ASIP Santé doivent être présents (se reporter au chapitre « Détails de certificat »).

Il peut donc y avoir jusqu'à **10** certificats « root » ASIP dans ce magasin.

L'import par fichier « P7B » est possible :

- **cer\p7b\01-prod-root.p7b**
  - 5 certificats de production
- **cer\p7b\03-test-root.p7b**
  - 5 certificats de test
- **cer\p7b\05-all-root.p7b**
  - 10 certificats de production et de test

Conseil : les certificats de test ASIP Santé doivent être supprimés des environnements de production

Conseil : ne pas utiliser le mécanisme Microsoft de sélection automatique du magasin de certificats lors de l'opération d'import !

Vérifier le magasin « Local machine \ intermédiaire » : Les certificats ASIP Santé intermédiaires doivent être présents.

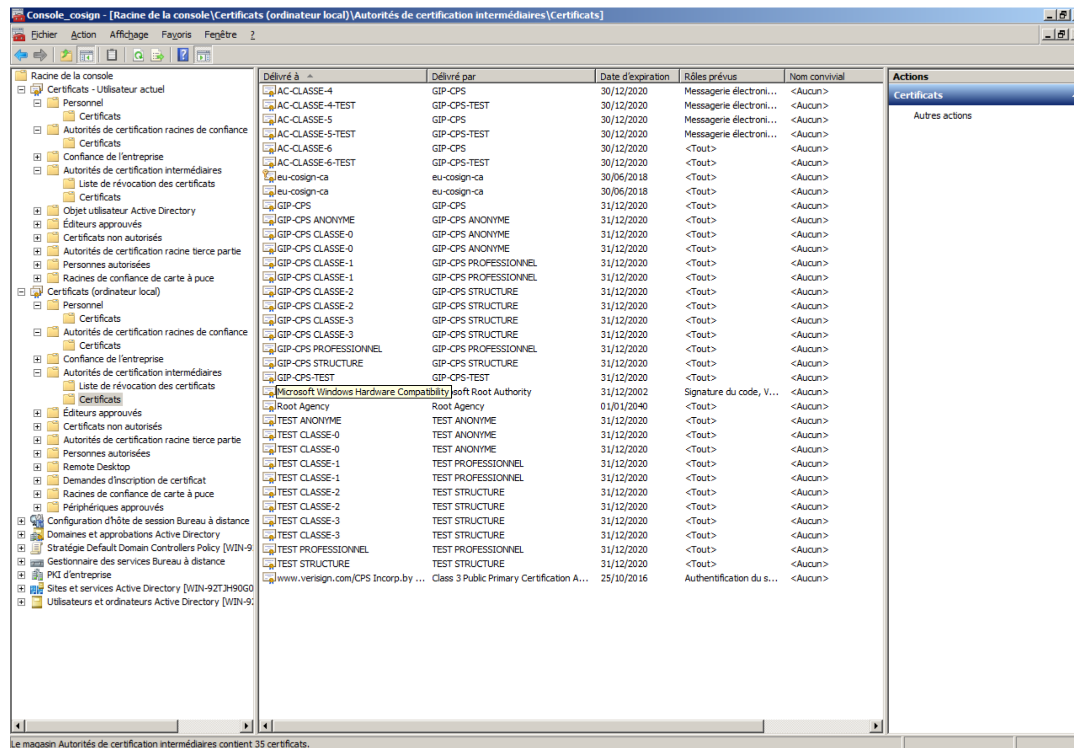


Figure 124 : CPSRev: vérification du magasin Intermediate CA (Local machine)

A minima, les 15 certificats intermédiaires de production de l'ASIP Santé doivent être présents.

Si des cartes de test sont utilisées (environnements de tests et d'homologation), les 15 certificats intermédiaires de test de l'ASIP Santé doivent être présents.

Il peut donc y avoir jusqu'à **30** certificats « intermédiaires » ASIP dans ce magasin.

L'import par fichier « P7B » est possible (et conseillé!):

- **cer\p7b\02-prod-inter.p7b**
  - 15 certificats de production
- **cer\p7b\04-test-inter.p7b**
  - 15 certificats de test
- **cer\p7b\06-all-inter.p7b**
  - 30 certificats de production et de test

Conseil : Se reporter au chapitre « Détails de certificat ») et imprimer ce tableau et matérialiser la vérification en cochant la case « Check »

Conseil : les certificats de test ASIP Santé doivent être supprimés des environnements de production

Conseil : ne pas utiliser le mécanisme Microsoft de sélection automatique du magasin de certificats lors de l'opération d'import !

Vérifier les magasins « Utilisateur actuel » :

Certificats racines :

Les certificats ASIP Santé racine doivent être présents, ils sont normalement provisionnés à partir du moment où le magasin « local machine » correspondant l'a correctement été (cf. étapes précédentes).

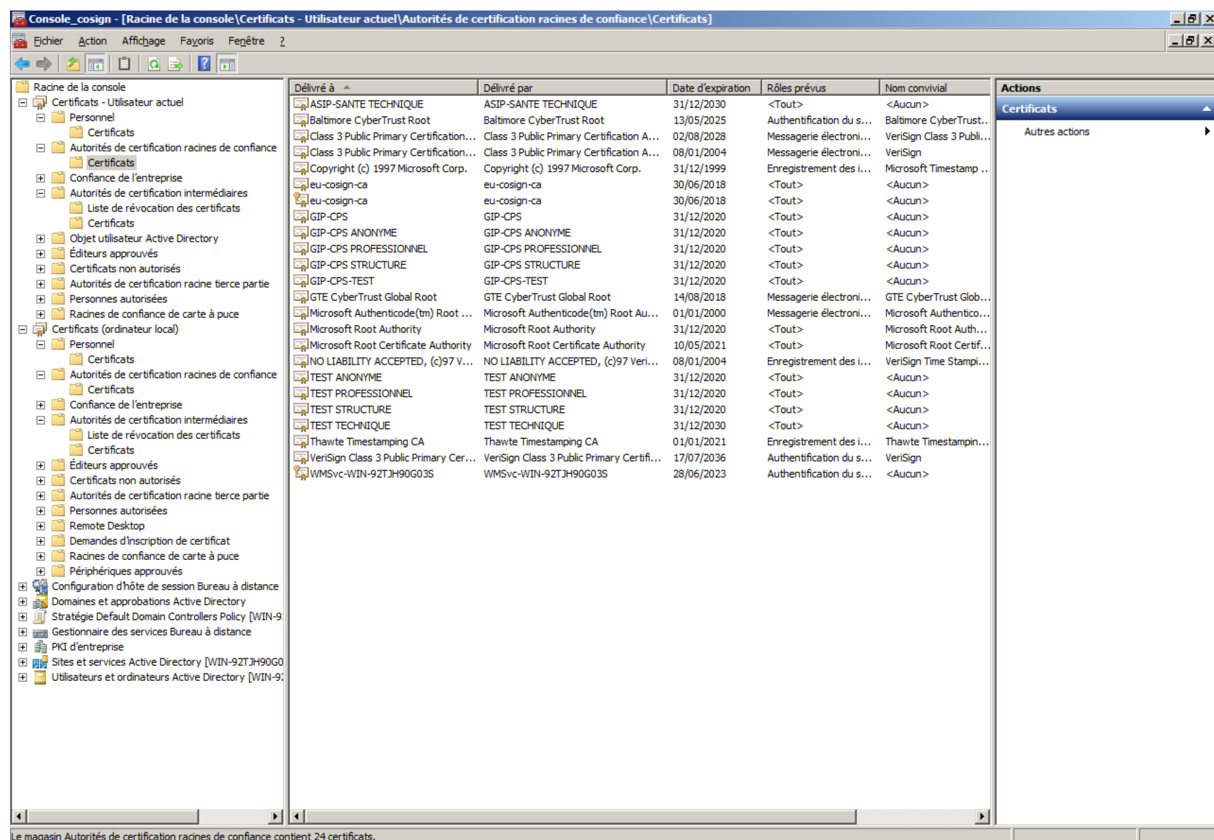


Figure 125 : CPSRev: vérification du magasin Root CA (User)

Certificats intermédiaires :

Les certificats ASIP Santé intermédiaires doivent être présents, ils sont normalement provisionnés à partir du moment où le magasin « local machine » correspondant l'a correctement été (cf. étapes précédentes).

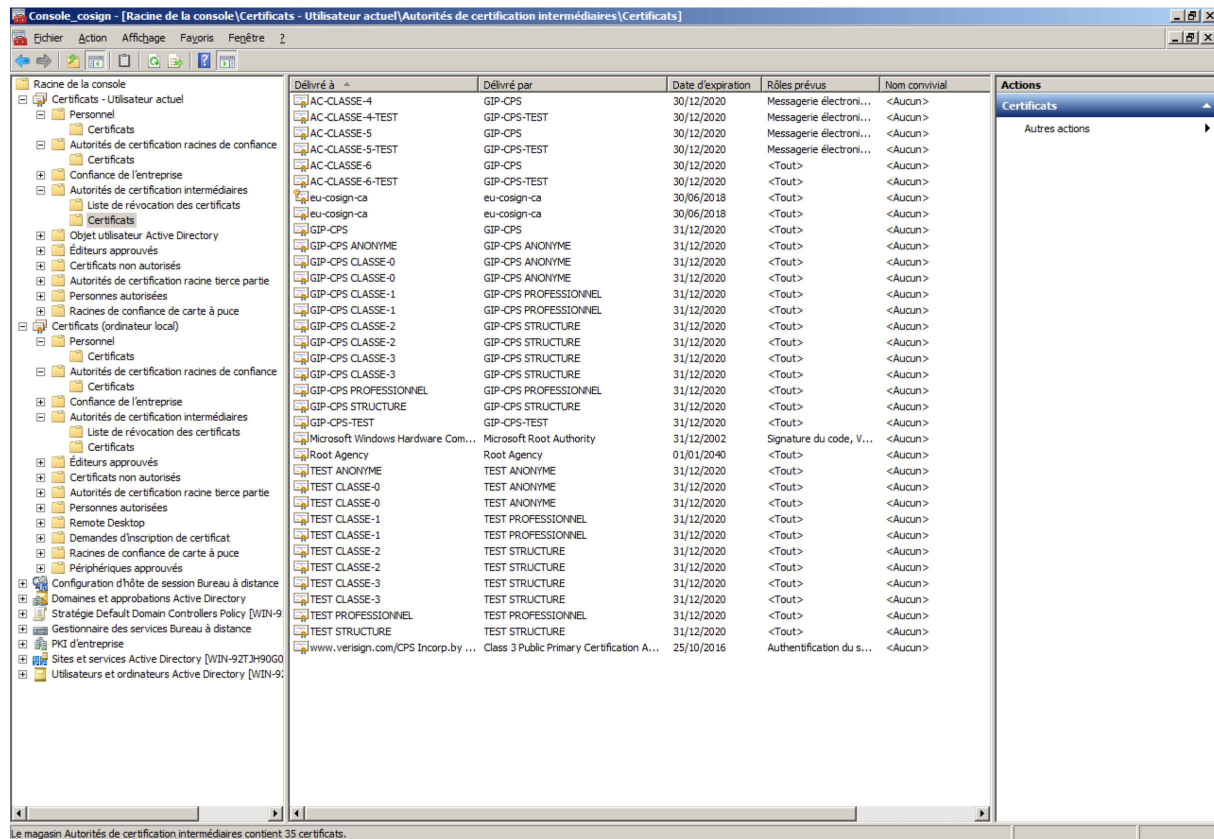


Figure 126 : CPSRev: vérification du magasin Intermediate CA (User)

Conseil : les certificats de test ASIP Santé doivent être supprimés des environnements de production

12.9.3 Configuration du Provider de révocation ASIP Santé – Microsoft

Mettre à jour la base de registre avec les paramètres CPSRev (cf. documentation du provider de révocation ASIP Santé), en particulier si des cartes de tests sont utilisées (prise en compte des cartes non GIP-CPS, les cartes de tests n'en étant pas pour des raisons de sécurité) :

```
; Configuration de CPSRev pour prendre en compte les certificats de test ASIP Santé:

[HKEY_LOCAL_MACHINE\SOFTWARE\GIPCPS\CPSRev]
"LogLevel"=dword:00000003
"WarnIfNotGIPCPSCert"=dword:00000001
"CheckAllCerts"=dword:00000001
"LogUndeterminatedAsError"=dword:00000001
```

Tableau 20 : CPSRev : Configuration de CPSRev pour prise en compte des certificats de test ASIP Santé

```
; Désactivation de la vérification des listes de révocation sous Win2008+

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters]
"UseCachedCRLOnlyAndIgnoreRevocationUnknownErrors"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kdc]
"UseCachedCRLOnlyAndIgnoreRevocationUnknownErrors"=dword:00000001
```

Tableau 21 : CPSRev : Désactivation de la vérification des listes de révocation sous Win2008+

```
; Activation de la vérification des listes de révocation sous Win2008+

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters]
"UseCachedCRLOnlyAndIgnoreRevocationUnknownErrors"=-

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kdc]
"UseCachedCRLOnlyAndIgnoreRevocationUnknownErrors"=-
```

Tableau 22 : CPSRev : (Ré-)Activation de la vérification des listes de révocation sous Win2008+

12.9.4 Cas des contrôleurs de domaine avec accès internet : vérification des statuts de certificats « online »

Vérifier les flux vers les serveurs ASIP avec IE :

Flux HTTP	http://annuaire.gip-cps.fr/crl/test/TEST%20CLASSE-2.crl
Flux LDAP	ldap://annuaire.gip-cps.fr/cn=test classe-2,ou=test structure,o=test,c=fr?certificaterevocationlist;binary

Tableau 23 : CPSRev : Vérification des flux vers l'annuaire ASIP Santé

Vérifier l'état d'un certificat carte d'authentification (extrait avec CPS Gestion ou avec inetcpl.cpl) **depuis le serveur** avec **certutil -verify -urlfetch**.

12.9.5 Cas des contrôleurs de domaine sans accès internet : vérification des statuts de certificats « offline » via l'alimentation du magasin de CRL en ligne de commande

Dans le cas – répandu – où les contrôleurs de domaine n'ont pas d'accès internet, il est nécessaire

1. de télécharger les CRLs ASIP Santé sur une machine dédiée
2. de les copier sur les contrôleurs de domaine
3. de les importer dans le magasin de liste de révocation

Cette dernière opération s'automatise avec l'outil certmgr.exe de Microsoft fourni avec Visual Studio. La ligne de commande est la suivante :

"certmgr.exe" -add -v -crl "chemin_du_fichier.crl" -s -r localMachine CA

Tableau 24 : CPSRev : Ligne de commande certmgr.exe

La documentation de certmgr.exe est ici : http://msdn.microsoft.com/en-us/library/e78byta0(v=vs.110).aspx

Le magasin est consultable visuellement en utilisant la mmc (autorité de certification intermédiaire > Liste de révocation des certificats):

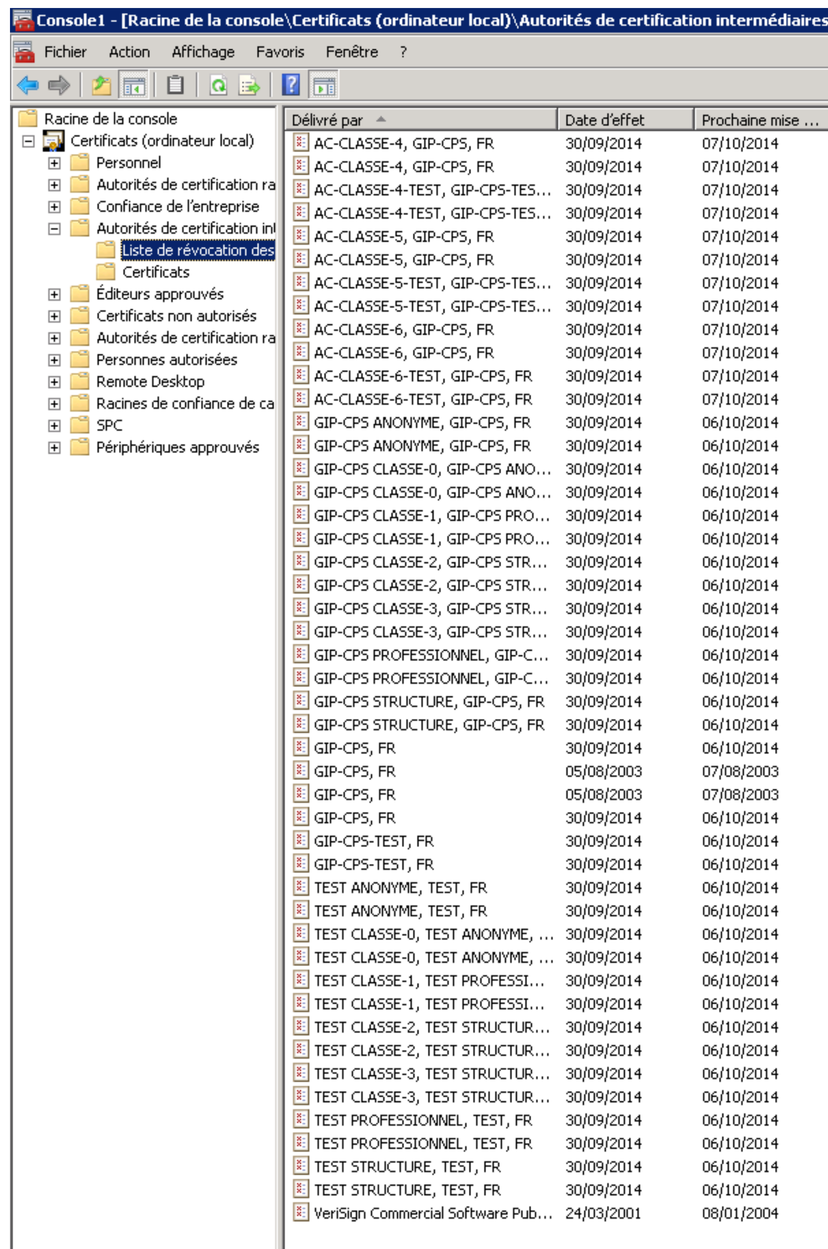


Figure 127 ; CPSRev : vérification des statuts de certificats offline : consultation du magasin de CRL

12.9.6 Test du Provider de révocation ASIP Santé – Microsoft en vérifiant le statut d'un certificat

Ex. : **certutil -verify -urlfetch 03-asipsante-cpsrev-test.cer**

Les messages renvoyés par certutil diffèrent entre une vérification « online » et une vérification « offline ».
Dans les 2 cas, le message « ***Vérification de révocation du certificat feuille réussie*** » final doit s'afficher.

```
Émetteur:
  CN=TEST CLASSE-2
  OU=TEST STRUCTURE
  O=TEST
  C=FR
Objet:
  CN=500000000018119/CPAT0001 + SN=RESPONSABLE0000018110001 + G=CHARLES
  OU=300000000018119
  L=Paris (75)
  O=TEST
  C=FR
Numéro de série du certificat : 4c8ddd

dwFlags = CA_VERIFY_FLAGS_CONSOLE_TRACE (0x20000000)
dwFlags = CA_VERIFY_FLAGS_DUMP_CHAIN (0x40000000)
ChainFlags = CERT_CHAIN_REVOCATION_CHECK_CHAIN_EXCLUDE_ROOT (0x40000000)
HCCE_LOCAL_MACHINE
CERT_CHAIN_POLICY_BASE
-------- CERT_CHAIN_CONTEXT --------
ChainContext.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100)
ChainContext.dwRevocationFreshnessTime: 17 Hours, 5 Minutes, 45 Seconds

SimpleChain.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100)
SimpleChain.dwRevocationFreshnessTime: 17 Hours, 5 Minutes, 45 Seconds

CertContext[0][0]: dwInfoStatus=102 dwErrorStatus=0
 Issuer: CN=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR
 NotBefore: 01/02/2013 02:00
 NotAfter: 29/02/2016 23:59
 Subject: CN=500000000018119/CPAT0001 + SN=RESPONSABLE0000018110001 + G=CHARLES, OU=300000000018119, L=Paris (75),
O=TEST, C=FR
 Serial: 4c8ddd
 SubjectAltName: Autre nom :Nom principal=5.00000000018119.CPAT0001@carte-cps.fr
 cc 8c f7 e3 0c 7b 6f 62 7f 66 76 5a 32 92 ac e1 a2 95 d7 65
 Element.dwInfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x2)
 Element.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100)
 ---------------- AIA de certificat ----------------
```

```
 Pas d'URL "Aucun" Heure : 0
 ----------------  CDP de certificat  ----------------
 Émetteur incorrect "Liste de révocation des certificats de base (108f)" Heure : 0
   [0.0] http://annuaire.gip-cps.fr/crl/test/TEST CLASSE-2.crl

 Émetteur incorrect "Liste de révocation des certificats de base (108f)" Heure : 0
   [1.0] ldap://annuaire.gip-cps.fr/cn=test classe-2,ou=test structure,o=test,c=fr?certificaterevocationlist;binary

 ----------------  CDP de liste de révocation des certificats de base  ----------------
 Pas d'URL "Aucun" Heure : 0
 ----------------  Protocole OCSP du certificat  ----------------
 Pas d'URL "Aucun" Heure : 0
 --------------------------------
   CRL 108f:
   Issuer: CN=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR
   91 77 d0 b2 82 bc 7d 55 36 8b 32 cb 1a 0c 4f 92 0b d2 e9 0e
   Delta CRL 108f:
   Issuer: CN=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR
   d5 34 f9 02 93 a9 c5 e6 56 21 01 76 14 33 5b 01 74 eb 88 2b
 Application[0] = 1.3.6.1.5.5.7.3.2 Authentification du client
 Application[1] = 1.3.6.1.4.1.311.20.2.2 Ouverture de session par carte à puce

CertContext[0][1]: dwInfoStatus=102 dwErrorStatus=0
 Issuer: OU=TEST STRUCTURE, O=TEST, C=FR
 NotBefore: 11/10/2004 02:00
 NotAfter: 31/12/2020 23:59
 Subject: CN=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR
 Serial: 1212
 54 df ee 1a c4 cd 8d 5a cf 32 f7 ae 12 1e f2 6a 33 8f f1 3d
 Element.dwInfoStatus = CERT_TRUST_HAS_KEY_MATCH_ISSUER (0x2)
 Element.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100)
 ----------------  AIA de certificat  ----------------
 Pas d'URL "Aucun" Heure : 0
 ----------------  CDP de certificat  ----------------
 Émetteur incorrect "Liste de révocation des certificats de base (108f)" Heure : 0
   [0.0] ldap://annuaire.gip-cps.fr/ou=test structure,o=test,c=fr?certificaterevocationlist;binary

 ----------------  CDP de liste de révocation des certificats de base  ----------------
 Pas d'URL "Aucun" Heure : 0
 ----------------  Protocole OCSP du certificat  ----------------
 Pas d'URL "Aucun" Heure : 0
 --------------------------------
   CRL 108f:
   Issuer: OU=TEST STRUCTURE, O=TEST, C=FR
```

```
   7f e1 a1 b9 19 0c 35 50 98 72 88 fa b6 6b ed 7c 81 33 de d1


CertContext[0][2]: dwInfoStatus=10c dwErrorStatus=0
  Issuer: OU=TEST STRUCTURE, O=TEST, C=FR
  NotBefore: 11/10/2004 02:00
  NotAfter: 31/12/2020 23:59
  Subject: OU=TEST STRUCTURE, O=TEST, C=FR
  Serial: 1201
  90 da 3e 6d 02 1f a3 78 d5 5c ee ea 3c e7 b8 2c a7 c8 75 6b
  Element.dwInfoStatus = CERT_TRUST_HAS_NAME_MATCH_ISSUER (0x4)
  Element.dwInfoStatus = CERT_TRUST_IS_SELF_SIGNED (0x8)
  Element.dwInfoStatus = CERT_TRUST_HAS_PREFERRED_ISSUER (0x100)
  ----------------  AIA de certificat  ----------------
  Pas d'URL "Aucun" Heure : 0
  ----------------  CDP de certificat  ----------------
  Pas d'URL "Aucun" Heure : 0
  ----------------  Protocole OCSP du certificat  ----------------
  Pas d'URL "Aucun" Heure : 0
  --------------------------------
  Issuance[0] = 1.2.250.1.71.3.7.9.2.0.0.1


Exclude leaf cert:
  b8 7e ab 1e de 9b 6d 71 f8 60 5e a4 4b 36 5c 3b 16 01 cd 22
Full chain:
  8a 22 b7 a5 66 c5 f8 e0 7f 9b 48 8b aa e2 f2 88 75 18 7e c0
------------------------------------
Stratégies d'émissions vérifiées: Aucun
Stratégies d'application vérifiées:
   1.3.6.1.5.5.7.3.2 Authentification du client
   1.3.6.1.4.1.311.20.2.2 Ouverture de session par carte à puce
Le certificat est un certificat d'entité de fin
Vérification de révocation du certificat feuille réussie
CertUtil: -verify La commande s'est terminée correctement.
```

Tableau 25 : CPSRev : Résultat de la vérification d'un certificat avec CPSRev

12.10 Configuration d'une console de composants enfichables dédiée au Smartcard logon

Il est particulièrement intéressant de « centraliser » les éléments à configurer dans une console unique.

Cette opération se fait de la façon suivante :

« **Démarrer > Exécuter > MMC** » :

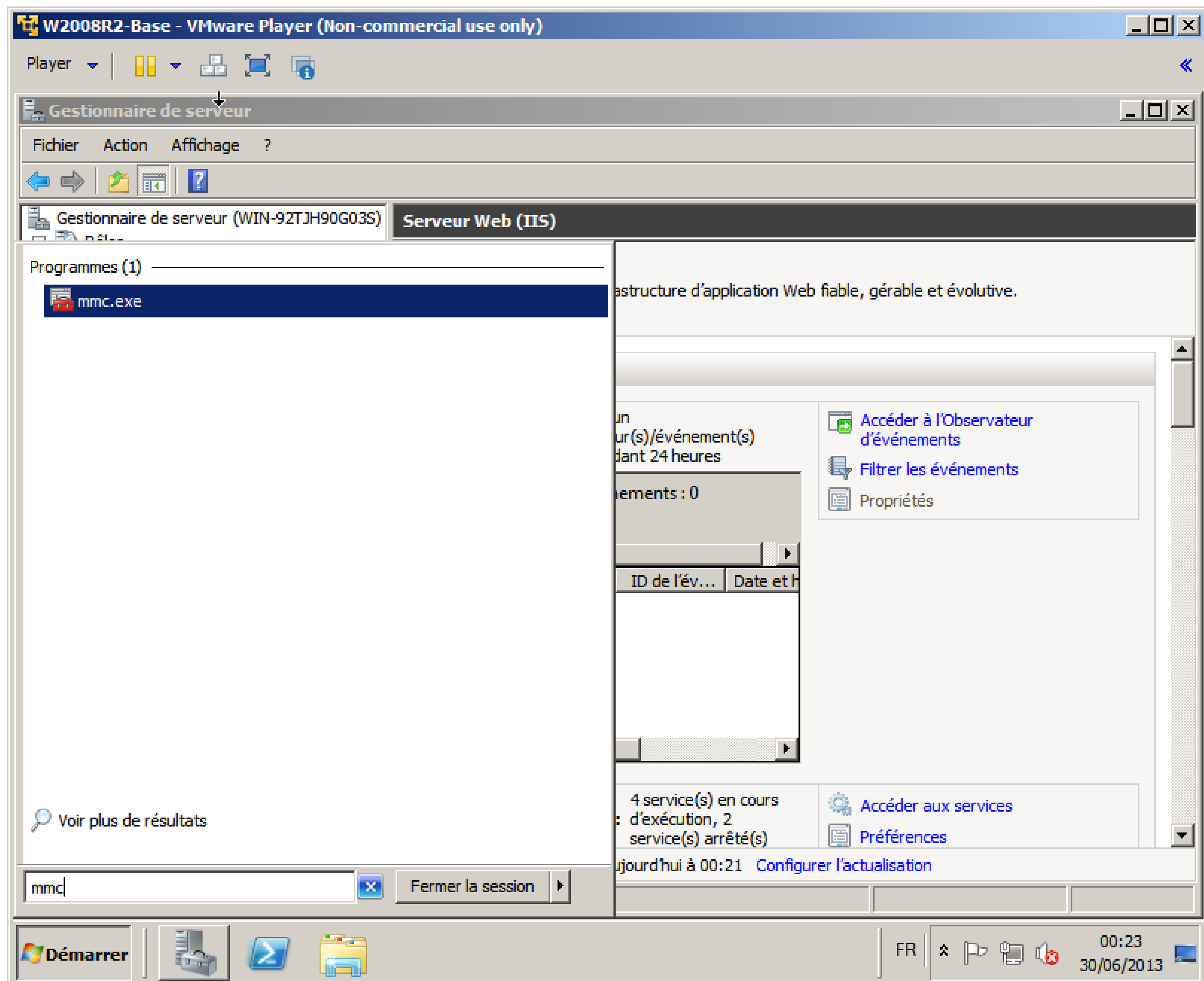


Figure 128 : Console Enfichable: MMC

Pour plus de rapidité, cliquer sur **« Fichier > Ouvrir... »** et choisir **bin/01-asipsante-console-smartcard-logon.msc** fourni dans le Pack.

Une fois cette console chargée, la quasi-totalité des éléments à configurer est disponible de façon centralisée.

Ce qui suit vous permet de composer des composants enfichables dans un fichier .msc « personnalisé ». Il n'est pas généralement pas nécessaire de suivre ce qui suit si **01-asipsante-console-smartcard-logon.msc** s'est correctement chargée.

« Fichier > Ajouter/Supprimer un composant enfichable... » :

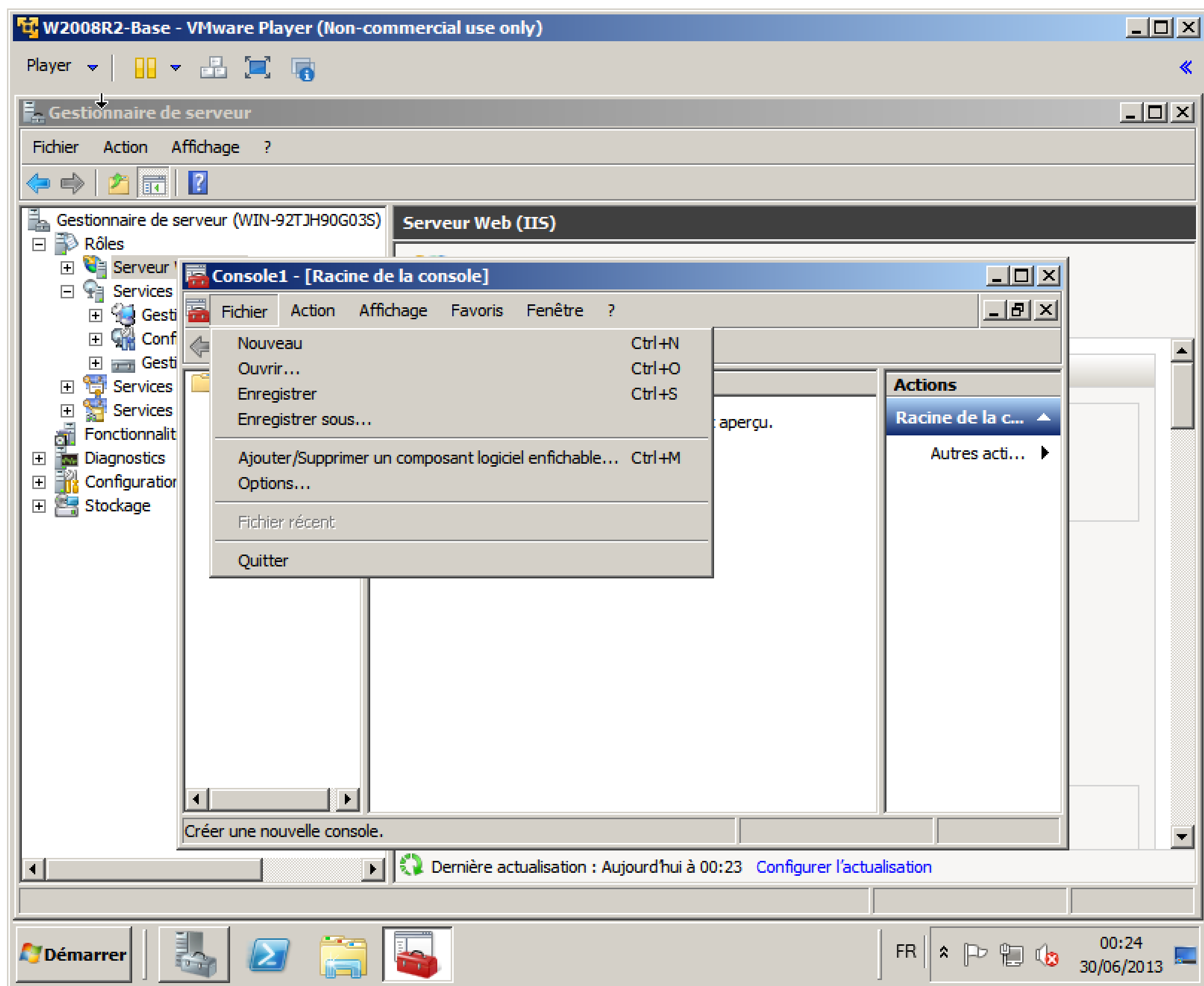


Figure 129 : Console Enfichable: Ajout de composants enfichables

« Certificats » :

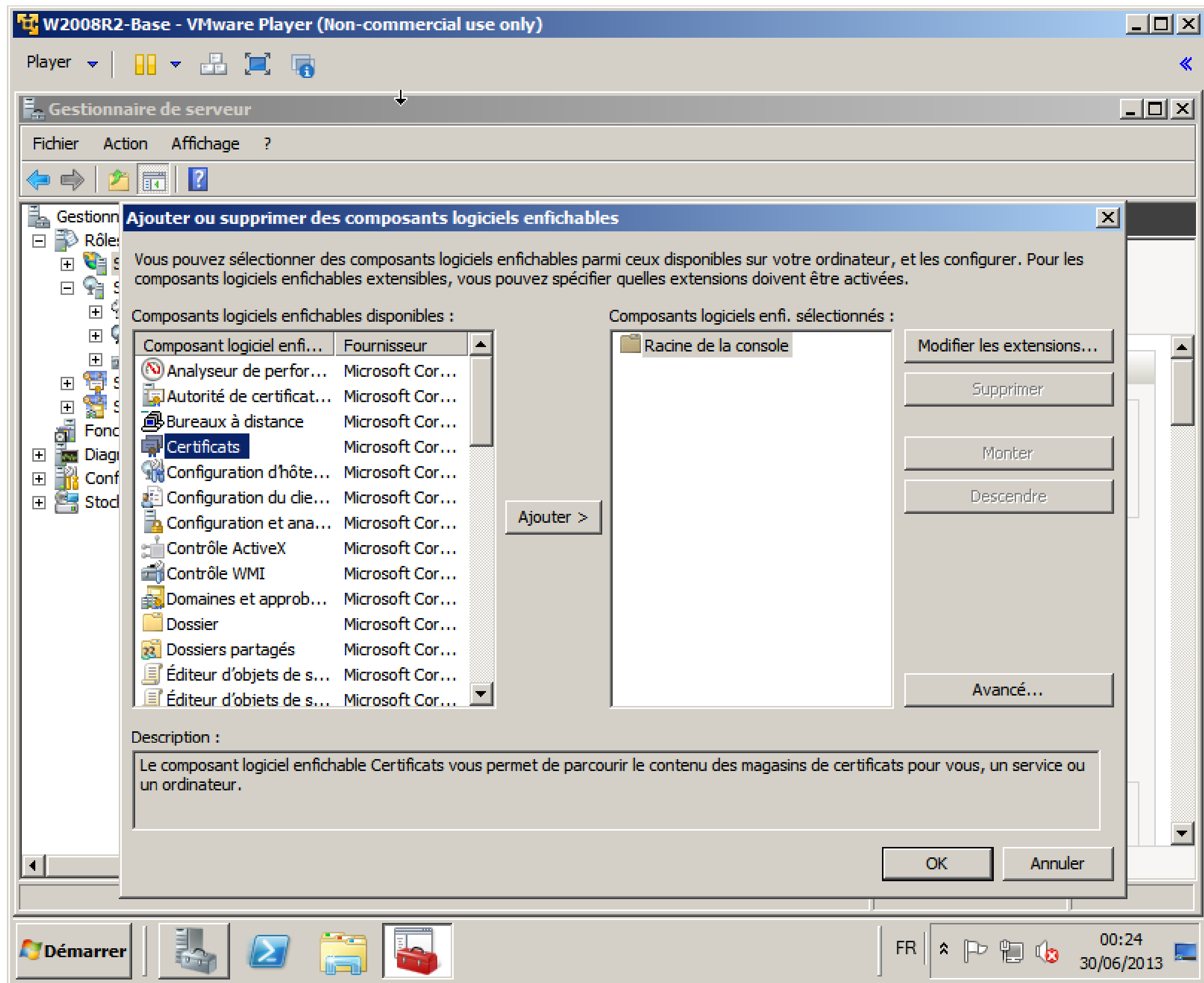


Figure 130 : Console Enfichable: Certificats

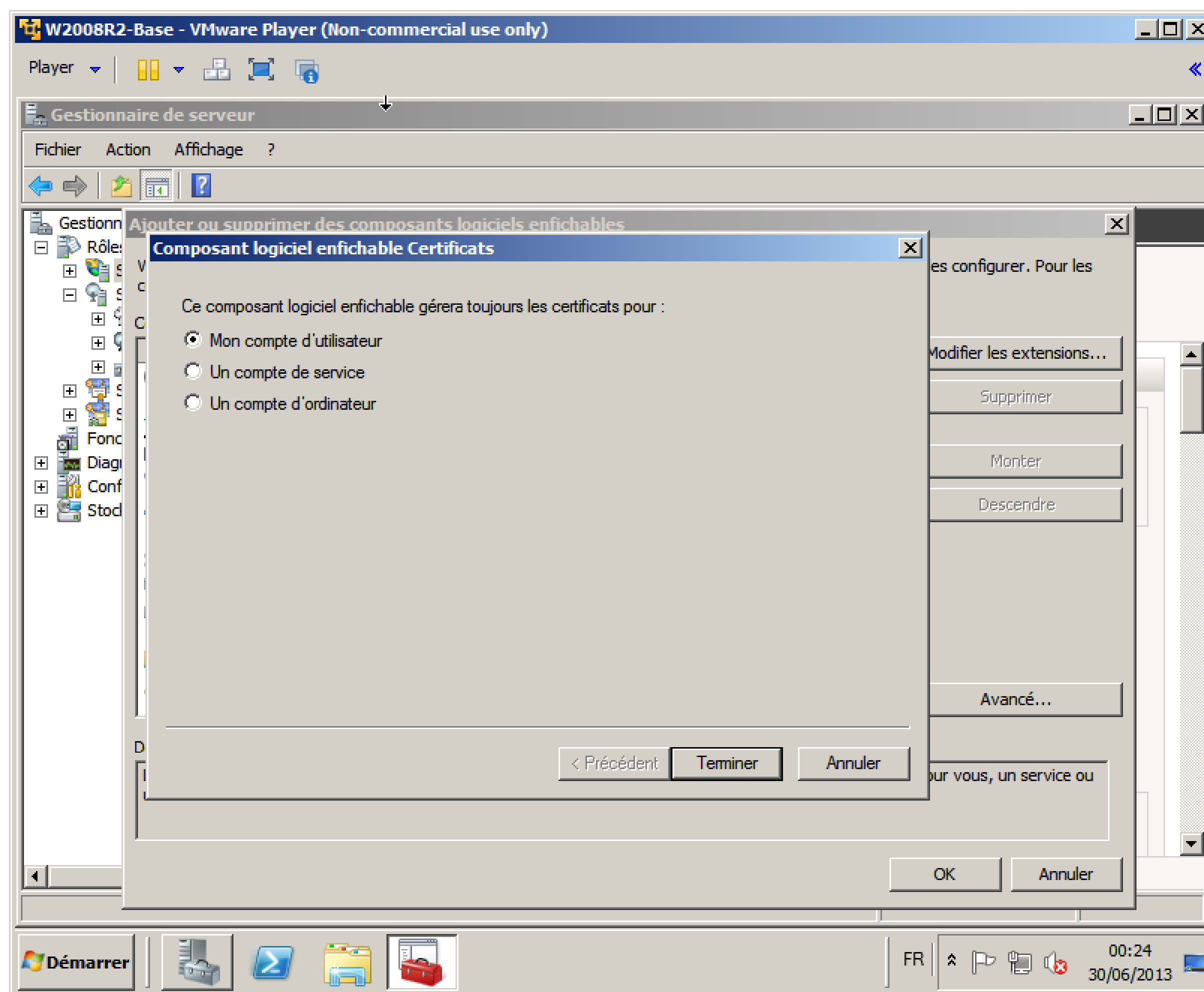


Figure 131 : Console Enfichable: Certificats utilisateur

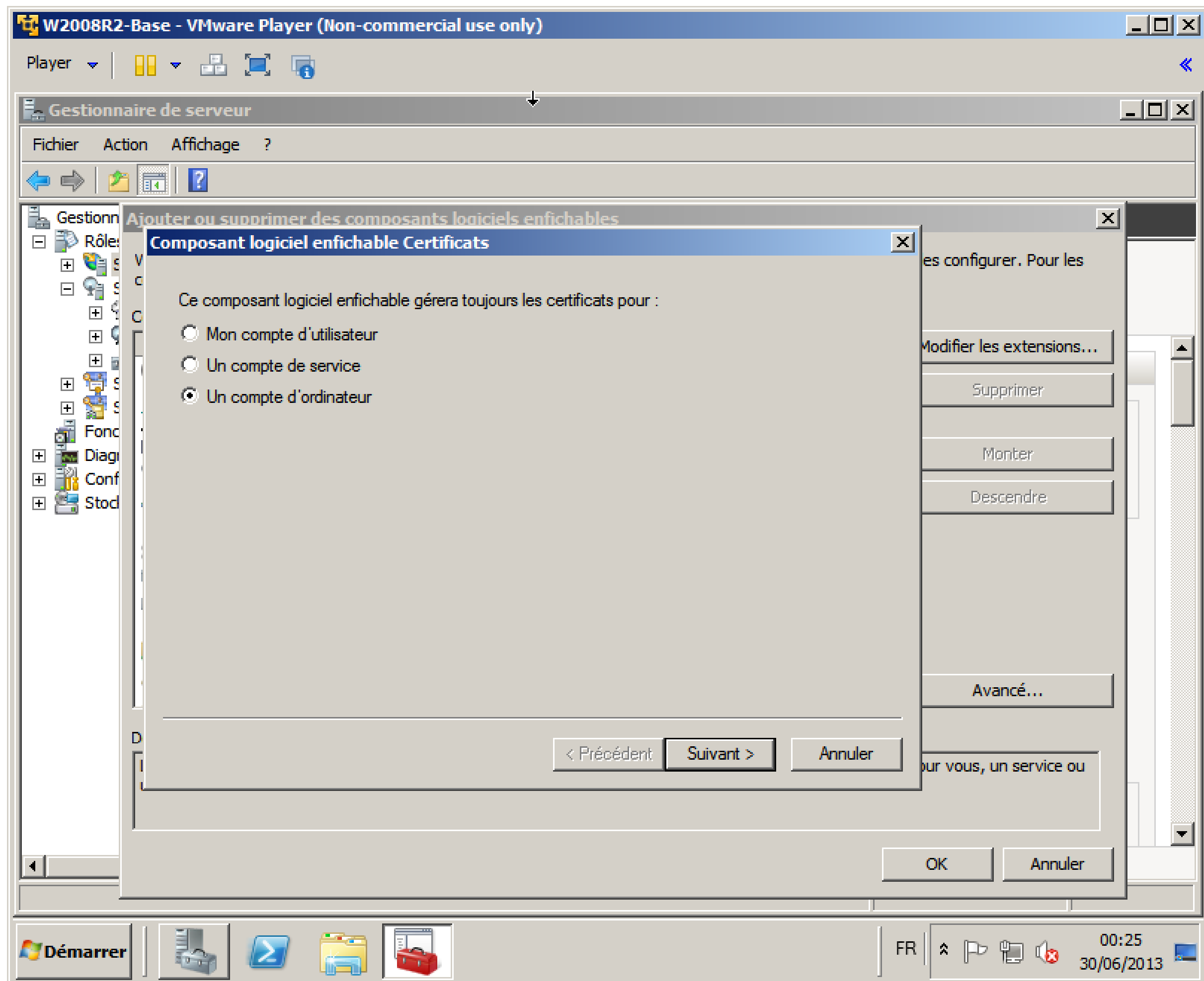


Figure 132 : Console Enfichable: Certificats Local Machine

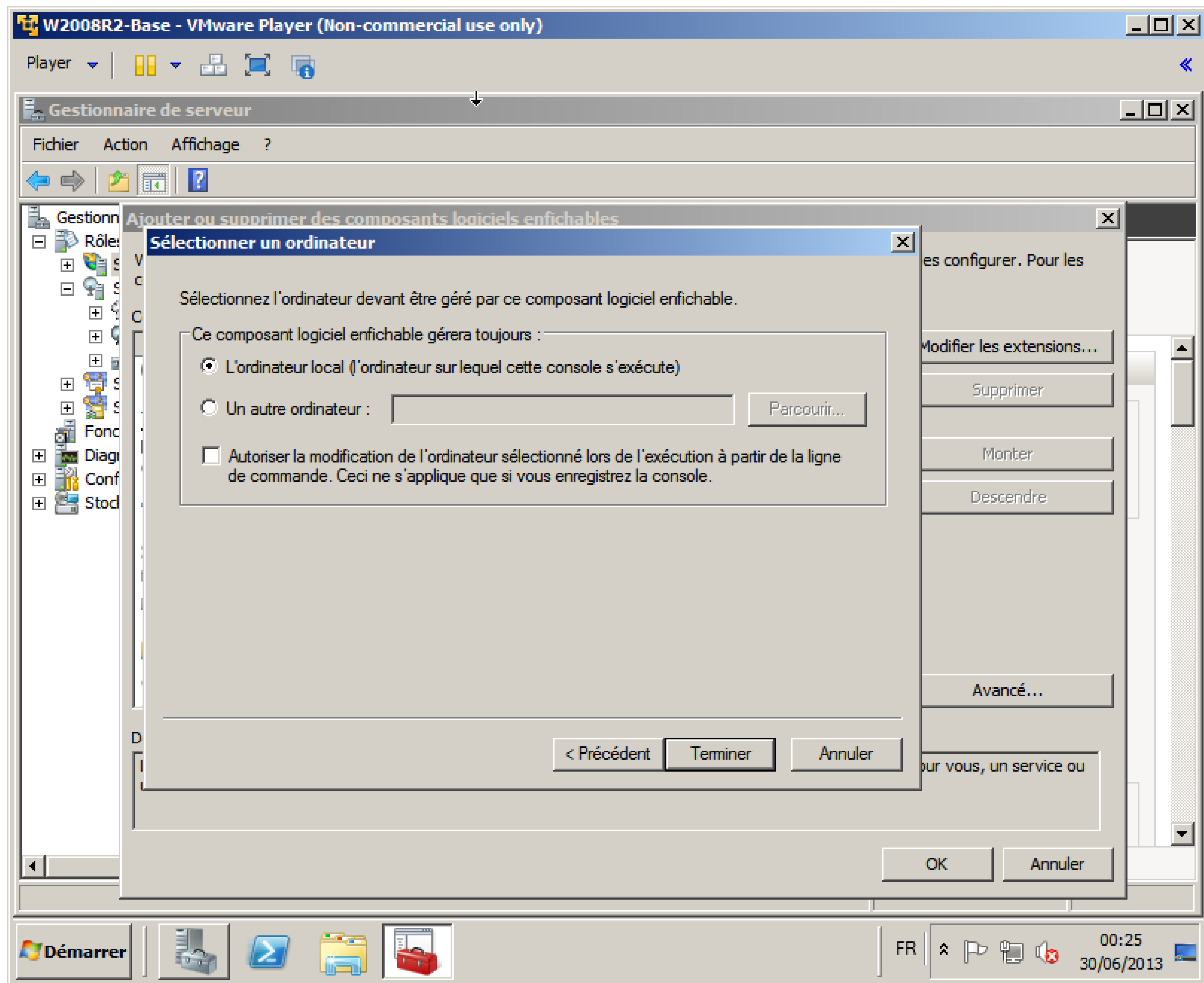


Figure 133 : Console Enfichable: Certificats Local Machine

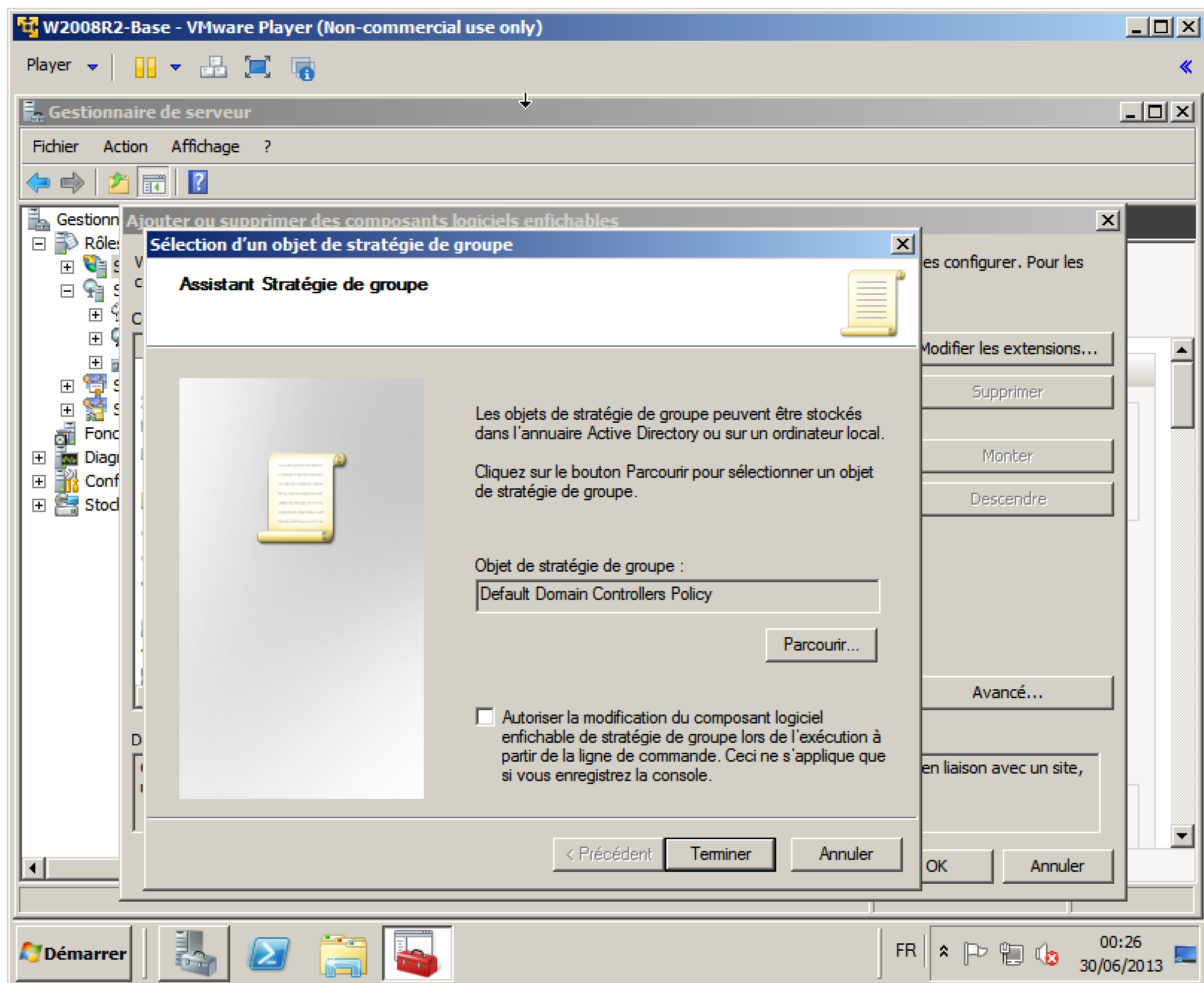


Figure 134 : Console Enfichable: Stratégie de groupe du contrôleur de domaine

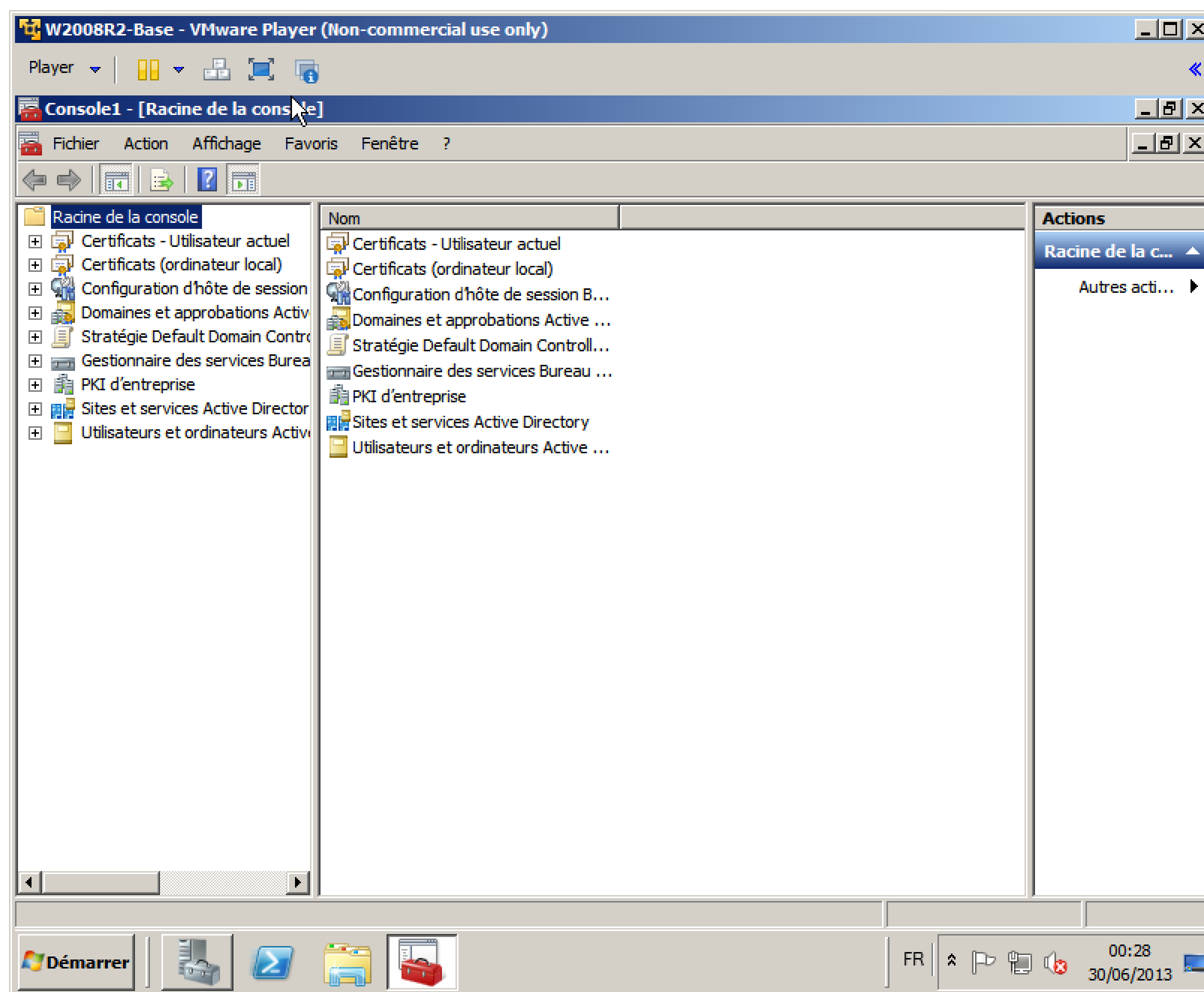


Figure 135 : Console Enfichable: Liste des composants utilisés pour le Smartcard logon

« **Fichier > Enregistrer sous…** » : choisir « **console-smartcard-logon.msc** » sur le bureau.

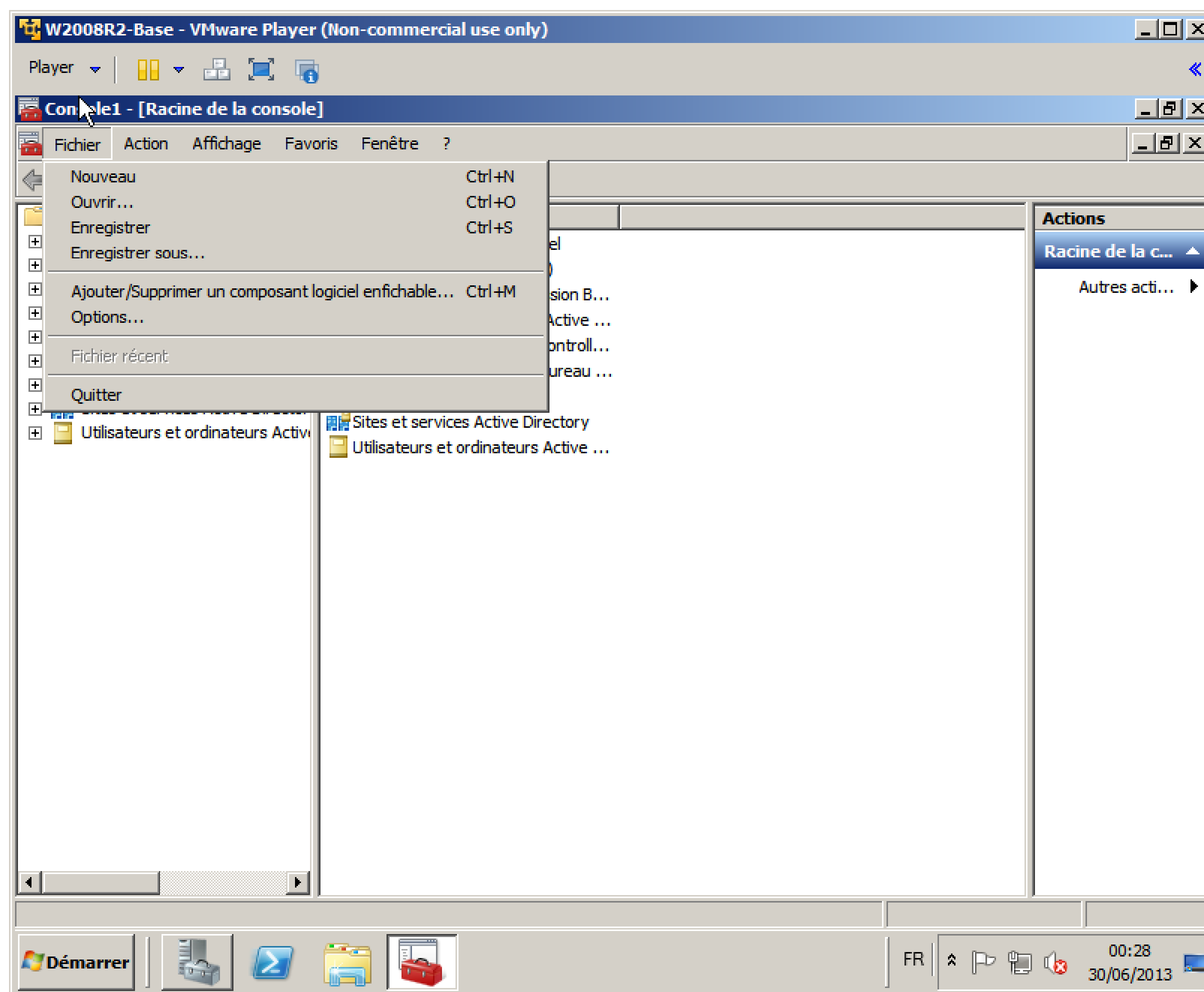


Figure 136 : Console Enfichable: Sauvegarde

12.11 Configuration du Contrôleur de domaine pour la Smartcard logon

12.11.1 Magasins de certificats

Commande MMC -> certificats -> **ordinateur local**

- Magasin **Personnel**
  - certificats racine
  - certificats DC (DomainController) du serveur
- Magasin **Autorités de certification racine de confiance**
  - certificats racine client
  - serveur
- Magasin **Autorités intermédiaires**
  - certificats client racine (signeur de CRL)
  - certificats intermédiaires client signeur de certificats et CRLs

En cas de contrôleurs de domaine multiple : installer ces certificats sur chaque contrôleur

12.11.1.1 Magasin personnel

Après installation de la Cryptolib CPS ou du provider de révocation, les certificats racine ne sont pas présents dans le magasin personnel (normal):

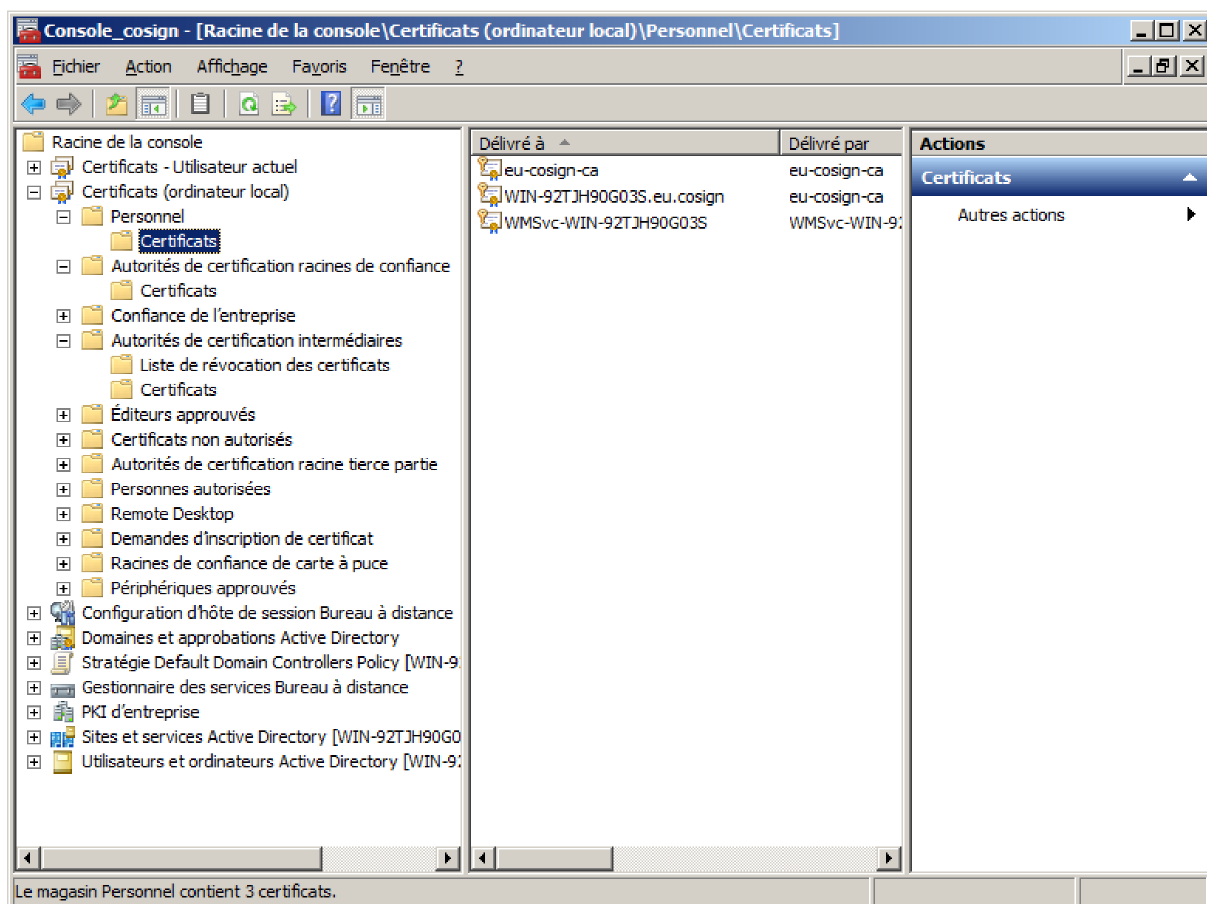


Figure 137 : Active Directory: Configuration: Certificat Local Machine personnel

Il est possible de les copier/coller depuis le magasin Root vers le magasin Personnel de l'ordinateur local :

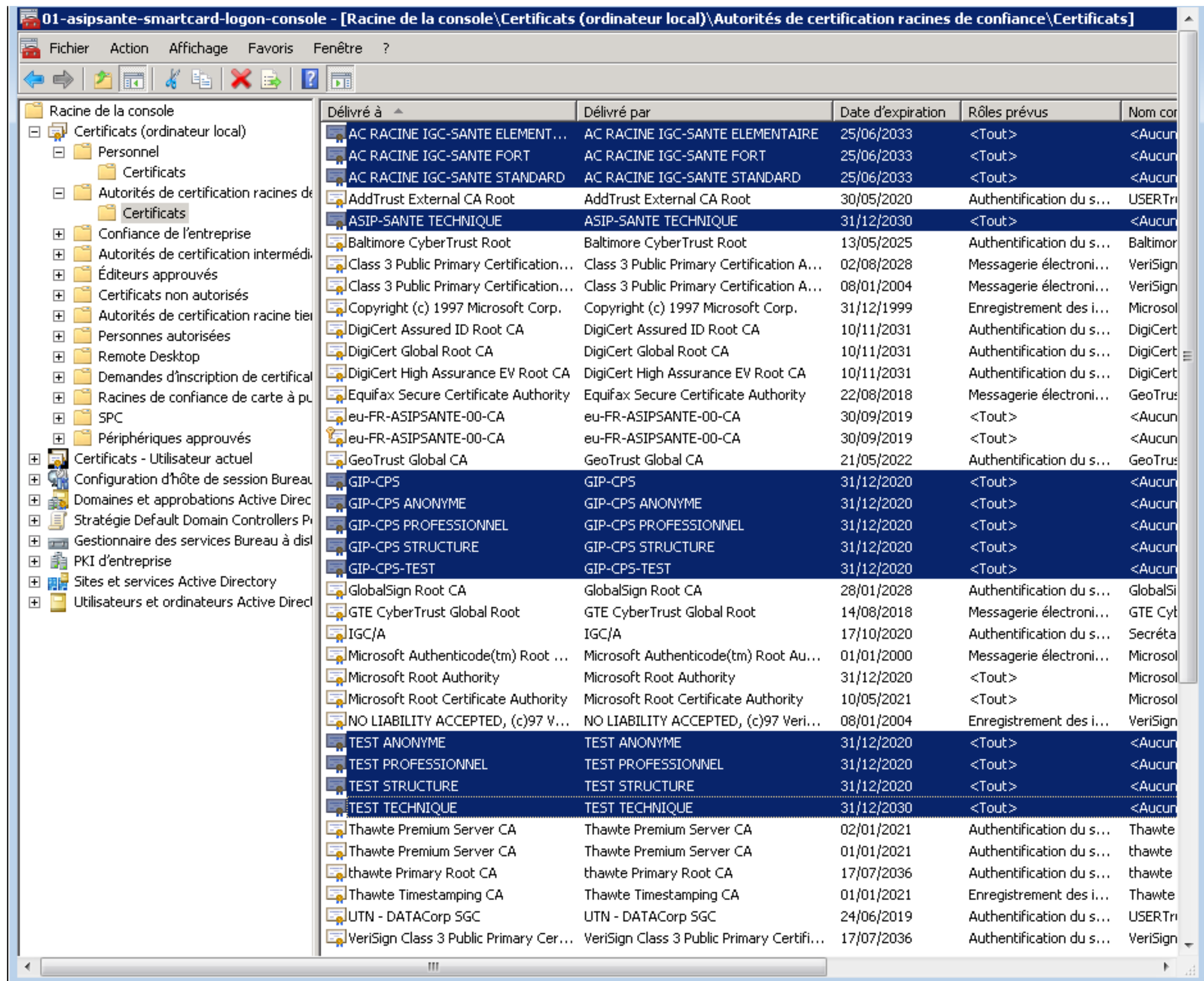


Figure 138 : Active Directory: Configuration: Copie de certificats Racine

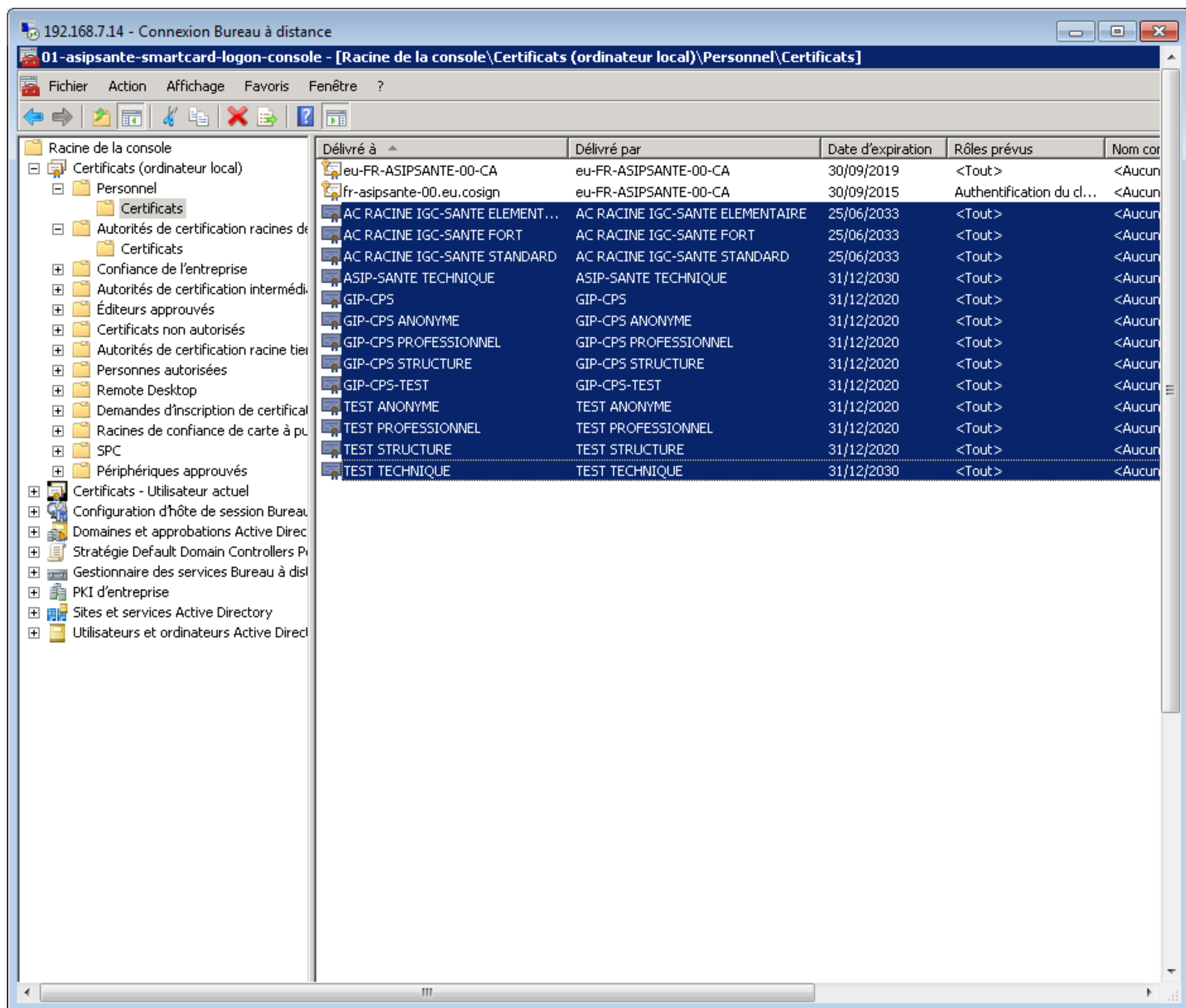


Figure 139 : Active Directory: Configuration: Collage de certificats Racine dans le magasin personnel

Le certificat racine « ASIP-SANTE TECHNIQUE » doit aussi être présent.

A minima, les 5 certificats root de production de l'ASIP Santé doivent être présents (les 5 root de l'IGC de santé de production actuelle).

Si des cartes de test sont utilisées (environnements de tests et d'homologation), les 5 certificats root de test de l'ASIP Santé doivent être présents.

Les **3** certificats root de production de la future IGC de santé peuvent être déployés.

Il peut donc y avoir jusqu'à **13** certificats « root » ASIP dans ce magasin.

L'import par fichier « P7B » est aussi possible :

- **cer\p7b\01-prod-root.p7b**
  - 8 certificats de production
- **cer\p7b\03-test-root.p7b**
  - 5 certificats de test
- **cer\p7b\05-all-root.p7b**
  - 13 certificats de production et de test

Conseil : Se reporter au chapitre « Détails de certificat » et imprimer le tableau et matérialiser la vérification en cochant la case « Check »

Conseil : les certificats de test ASIP Santé doivent être supprimés des environnements de production

12.11.1.2 Magasins Certificats Racine et intermédiaires

Cf. CPSRev.

S'assurer que le certificat racine de l'AD CS est provisionné dans la magasin racine (fait par défaut sur l'AD CS est sur le contrôleur de domaine).

12.11.1.3 Magasin NTAuth

Ajout des certificats d'autorités **client** (**racine + intermédiaire**) + **serveur** (racine) dans le magasin **NTAuth**.:

« MMC -> PKI d'entreprise -> Clic droit -> gérer les conteneurs Active Directory -> Conteneur NTAuthCertificates -> Ajouter »

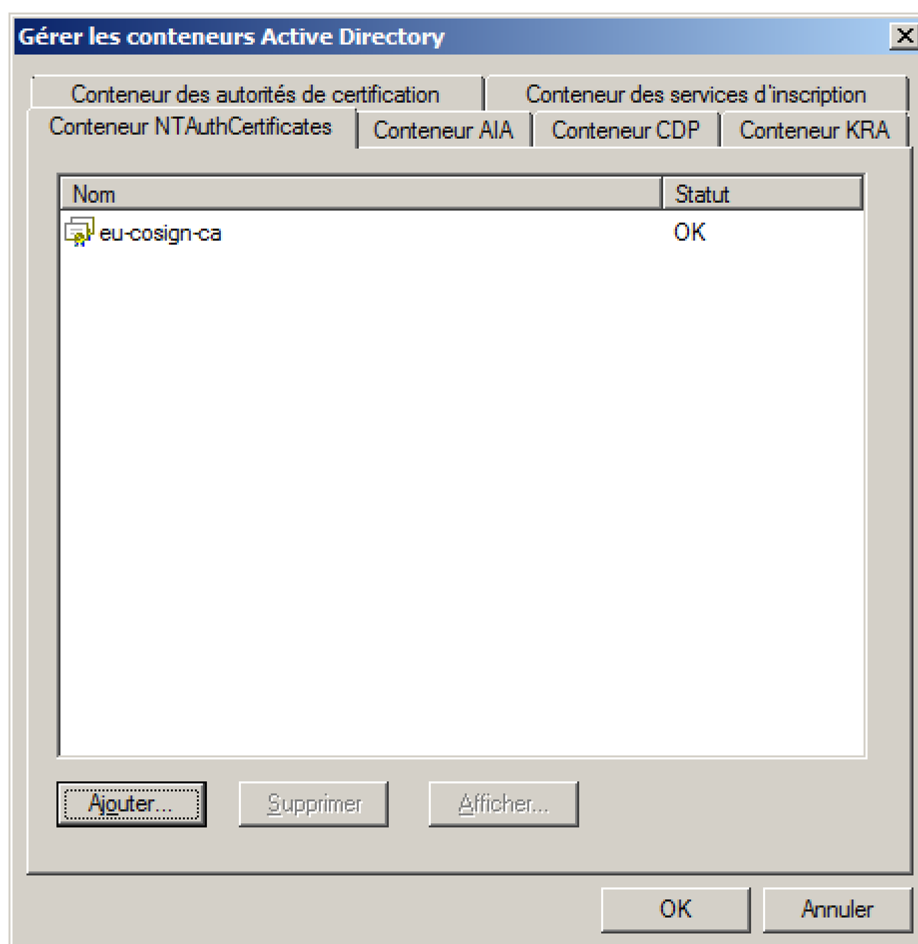


Figure 140 : Active Directory: Configuration: Magasin NTAUTH avant import

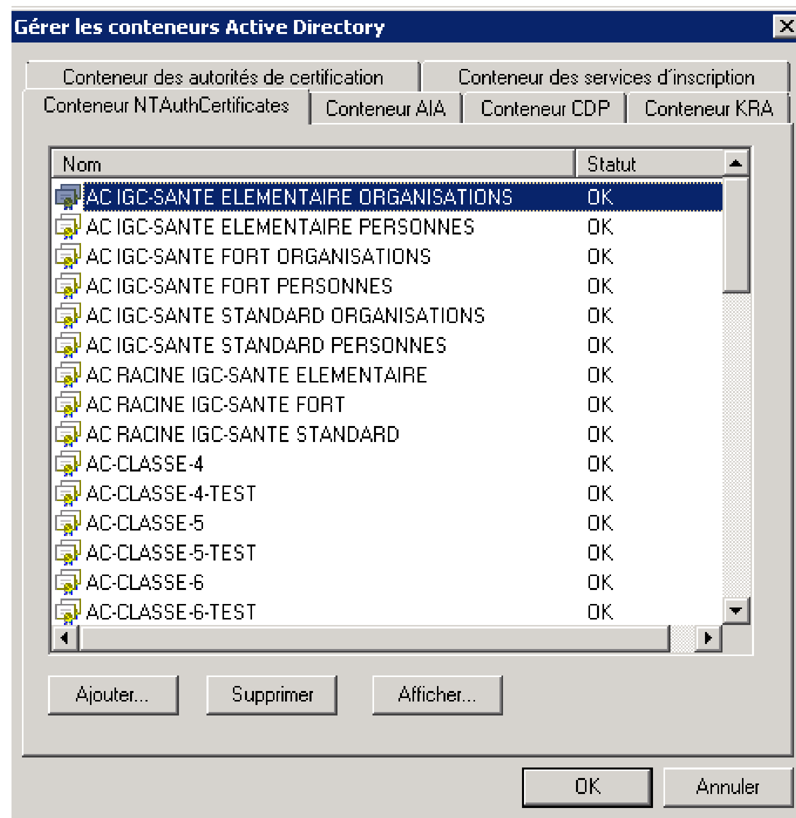


Figure 141 : Active Directory: Configuration: Magasin NTAUTH après import

- ⇨ 49 certificats au format .cer à importer 1 à 1
  - 40 certificats ASIP Santé
    - 20 de test
      - 5 root, 15 intermédiaires
    - 20 de production
      - 5 root, 15 intermédiaires
  - 9 certificats correspondants à la future IGC de santé
    - 9 de production
      - 3 root, 6 intermédiaires
  - fournis dans le répertoire **cer\cer**,
- ⇨ 1 certificat Autorité de certification AD CS

A minima:

1. **les 5 certificats racine de l'IGC de production actuelle de l'ASIP Santé**
2. **les 15 certificats intermédiaires de l'IGC de production de actuelle l'ASIP Santé**
3. **les 9 certificats (3 roots + 6 intermédiaires) de la future IGC de production l'ASIP Santé**
4. **le certificat du l'autorité de certification de l'AD CS**

doivent être présents.

Si des cartes de test sont utilisées (environnements de tests et d'homologation), les 5 certificats racines et les 15 certificats intermédiaires de test de l'ASIP Santé doivent être présents.

Il peut donc y avoir jusqu'à **49** certificats ASIP dans ce magasin et **1** certificat AD CS.

L'import par fichier « P7B » n'est pas possible, 2 choix s'offrent à nous:

- import un à un des certificats au format .cer
  - source d'erreur!
- import par fichier batch
  - vivement conseillé !
  - cf. script **bin\00-asipsante-smartcard-logon-ntauth-manage.cmd** fourni

La commande qui permet d'automatiser cet import est:

```
certutil -dspublish -f "fichier_certificat_a_importer.cer" NTAuthCA
```

Tableau 26 : Active Directory: Configuration: Commande certutil d'import des certificats dans le magasin NTAUTH

Conseil : Se reporter au chapitre « Détails des certificats ASIP Santé », imprimer ce tableau et matérialiser la vérification en cochant la case « Check »

Conseil : les certificats de test ASIP Santé doivent être supprimés des environnements de production

12.11.2 Stratégie Active Directory

12.11.2.1 Ajout des autorités racines client et serveur

« MMC -> Default Domain Controllers policy -> Configuration ordinateur -> Stratégies -> Paramètres Windows -> Paramètres de sécurité -> Stratégie de clé publique -> Autorité de certification racines de confiance -> importer »

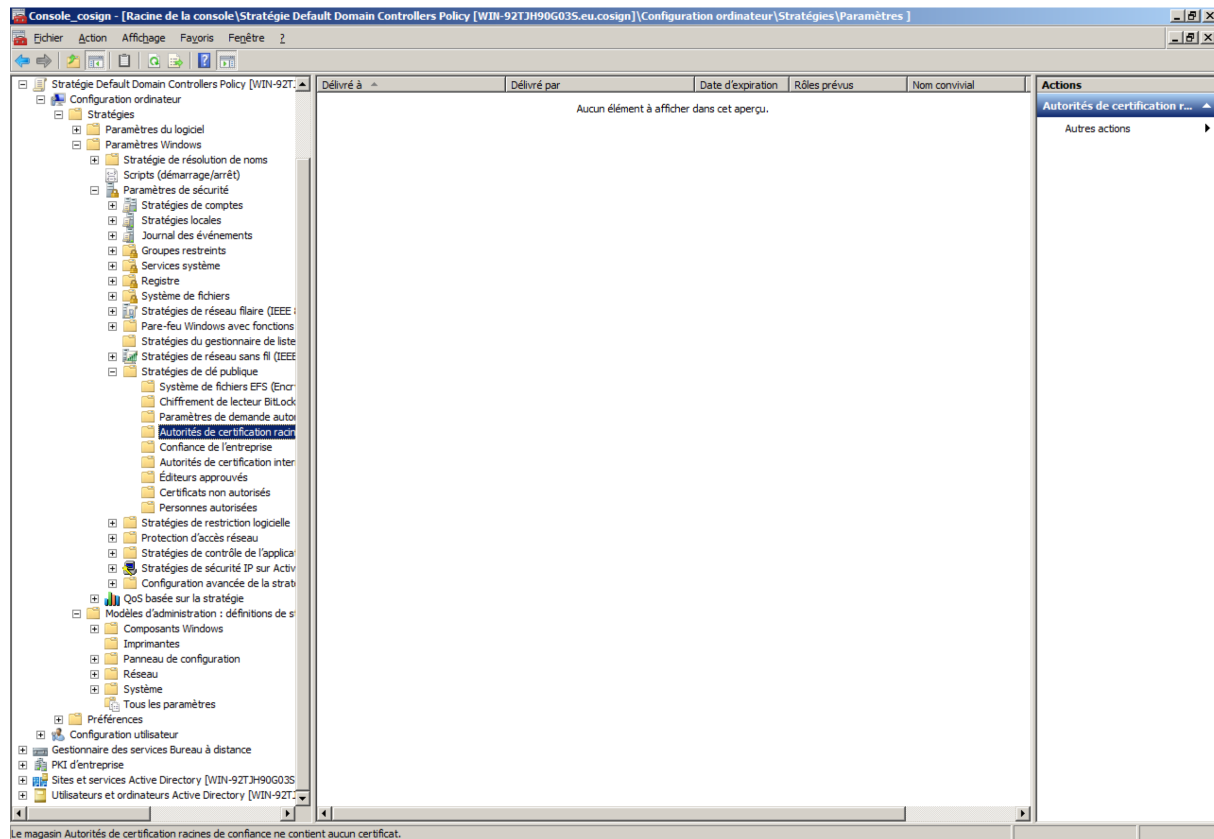


Figure 142 : Active Directory: Configuration: Stratégie de clé publique avant import

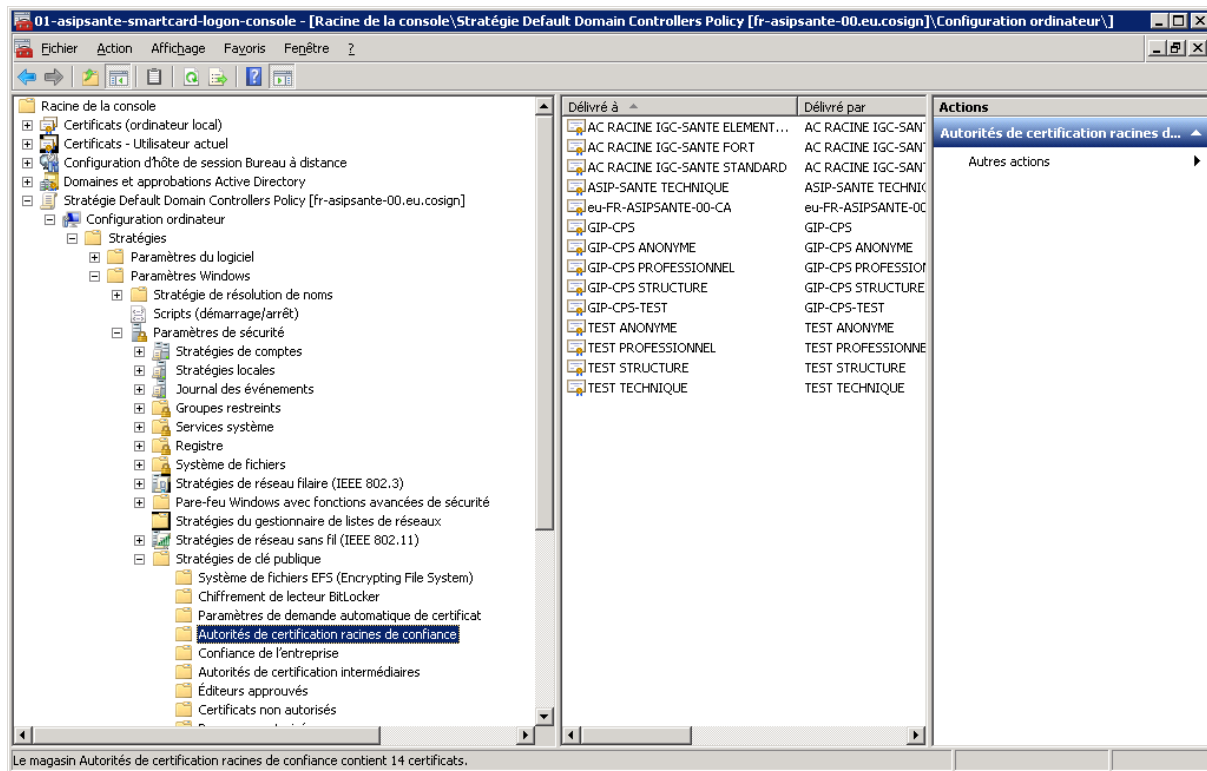


Figure 143 : Active Directory: Configuration: Stratégie de clé publique après import

A minima:

1. **les 5 certificats racine de l'IGC de production actuelle de l'ASIP Santé**
2. **les 3 certificats racine de la future IGC de production de l'ASIP Santé**
3. **le certificat du l'autorité de certification de l'AD CS**

Doivent être présents.

Si des cartes de test sont utilisées (environnements de tests et d'homologation), les 5 certificats racines de l'ASIP Santé doivent être présents.

Il peut donc y avoir jusqu'à **13** certificats ASIP dans ce magasin et **1 certificat AD CS**.

L'import par fichier « P7B » est possible :

- **cer\p7b\01-prod-root.p7b**
  - 8 certificats de production
- **cer\p7b\03-test-root.p7b**
  - 5 certificats de test
- **cer\p7b\05-all-root.p7b**
  - 13 certificats de production et de test

Conseil : Se reporter au chapitre « Détails de certificat », imprimer le tableau et matérialiser la vérification en cochant la case « Check »

Conseil : les certificats de test ASIP Santé doivent être supprimés des environnements de production

12.11.2.2 Ajout des autorités intermédiaires client et serveur

[3] page 17 point 13 stipule de compléter l'action précédente par :

« MMC -> Default Domain Controllers policy -> Configuration ordinateur -> Stratégies -> Paramètres Windows -> Paramètres de sécurité -> Stratégie de clé publique -> Autorité de certification intermédiaire -> importer »

Dans une configuration « de base », cette opération n'est apparemment pas nécessaire. Elle peut l'être sur une infrastructure complexe.

12.12 Création des utilisateurs

12.12.1 Construction de l'identifiant UPN

L'UPN (Universal Principal Name) est un identifiant unique présent dans le certificat d'authentification de la carte CPS (depuis Mars 2011) qui sert à faire le lien avec un compte utilisateur dans un annuaire Active Directory sur un contrôleur de domaine.

Cet UPN est construit de la manière suivante: **préfixeUPN@suffixeUPN**

Le **préfixeUPN** est la partie identifiant de manière unique la carte CPS.

- Il est construit de la manière suivante :
- Format : <Type d'identifiant>.<Id registre national>.<Id registre structure>
- Données correspondants au champ « CN » (= identifiant professionnel et personnel de santé) du champ « Objet » présent dans les certificats de la carte CPS.
- Cet identifiant PS est aussi inscrit physiquement sur le recto de la carte CPS, sur la première ligne imprimée sous la puce électronique.
- Un point est rajouté en deuxième position, pour séparer le premier chiffre (code du type d'identifiant PS sur un caractère), du reste de l'identifiant PS.
- Un point remplace chaque caractère spécial de cet identifiant PS.
- L'identifiant sur le registre de la structure est optionnel (en fonction du type d'identifiant).

Le **suffixeUPN** correspond à un nom de domaine générique géré par l'ASIP Santé

- il est fixe
- il a pour valeur : **carte-cps.fr**

Exemples d'UPN:

identifiant PS	CN	UPN
numéro de SIRET (code '5') + numéro de registre (numéro interne à la structure)	51871275100020/0000000137	5.18751275100020.0000000137@carte-cps.fr
numéro FINESS (code '3') + numéro de registre structure	30B0018289/CPET0003	3.0B0018289.CPET0003@carte-cps.fr
numéro ADELI (code '0')	00B6010140	0.0B6010140@carte-cps.fr
numéro RPPS (code '8')	899700011143	8.99700011143@carte-cps.fr

Tableau 27 : Déploiement UPN : Construction de l'UPN

12.12.3 Déclaration du suffixe carte-cps.fr dans l'AD

Si le suffixe de l'UPN n'apparait pas dans la liste des noms de domaines connus, une relation d'approbation avec le domaine existant devra préalablement être créée:

Outils d'administration -> **Domaines et approbations Active Directory.**

Pour ajouter une approbation au domaine existant, cliquer droit sur « **Domaines et approbations Active Directory »** puis choisir **« Propriétés »** et ajouter « **carte-cps.fr** »:

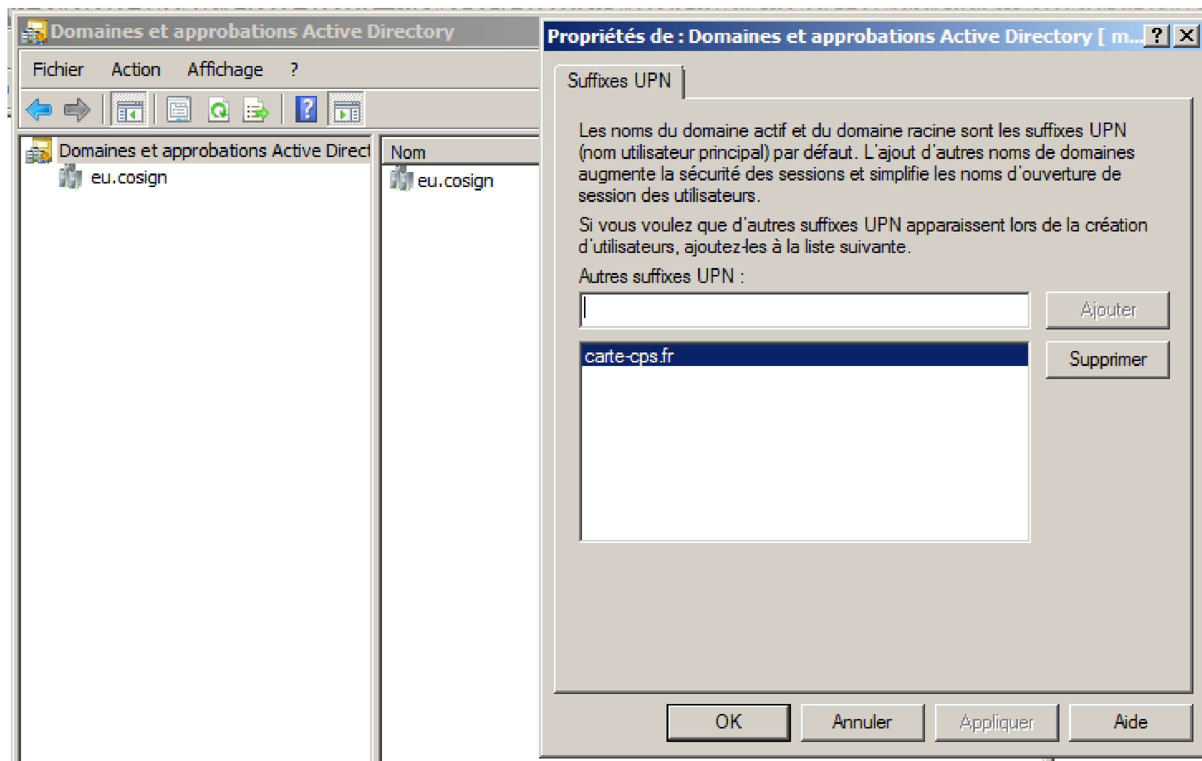


Figure 144 : Active Directory: Configuration: Approbation du suffixe UPN « carte-cps.fr »

12.12.4 Déclaration d'un utilisateur

Un nouvel utilisateur se déclare de la façon suivante dans l'AD :

Nouvel objet - Utilisateur

Créer dans : eu.cosign/Users

Prénom : Carte1 Initiales :

Nom :

Nom complet : Carte1

Nom d'ouverture de session de l'utilisateur :

0.0B1055421 @carte-cps.fr

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :

cosign\ Carte1

< Précédent Suivant > Annuler

Figure 145 : Active Directory: Configuration: Définition d'un compte avec Smartcard logon activé

Nouvel objet - Utilisateur

Créer dans : eu.cosign/Users

Mot de passe : ••••••••••

Confirmer le mot de passe : ••••••••••

☐ L'utilisateur doit changer le mot de passe à la prochaine ouverture de session

☐ L'utilisateur ne peut pas changer de mot de passe

☑ Le mot de passe n'expire jamais

☐ Le compte est désactivé

< Précédent Suivant > Annuler

Figure 146 : Active Directory: Configuration: Définition d'un compte avec Smartcard logon activé

Prêter attention à bien spécifier le domaine **carte-cps.fr**.

⇨ Voir annexe sur l'UPN
⇨ Voir figure « **Active Directory: Approbation du suffixe UPN « carte-cps.fr »** »

Si ce compte fait du Smartcard logon en TSE, se reporter à la section Terminal Serveur pour l'autorisation d'ouverture de session TSE associée.

⇨ Voir annexe sur le service de bureau à distance si le bureau à distance est utilisé (groupe et stratégie AD)

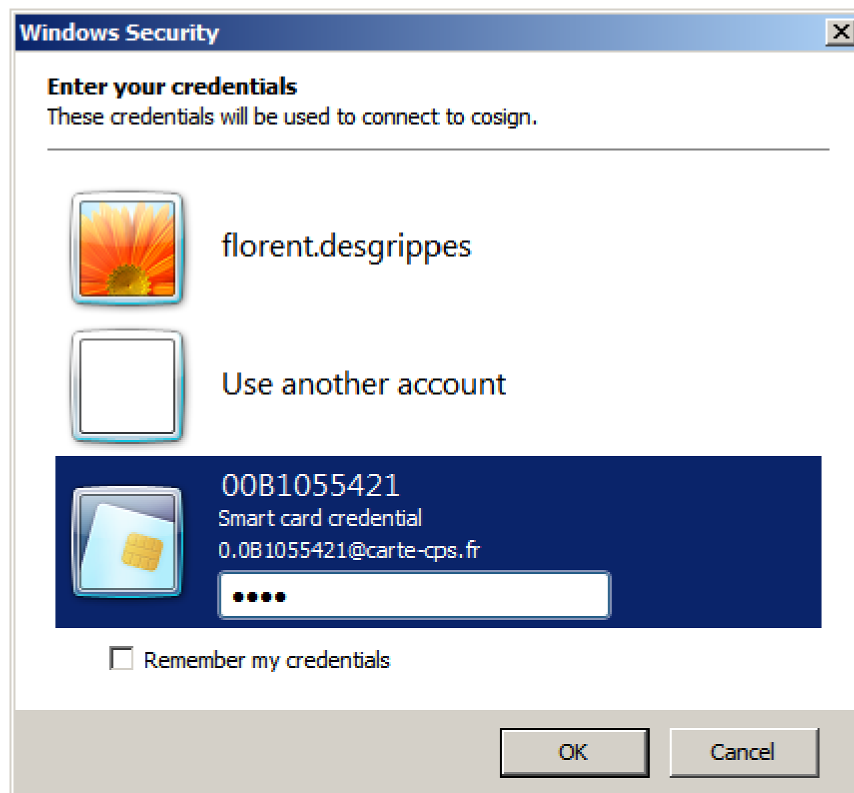


Figure 147 : Active Directory: Configuration: Smartcard logon en TSE

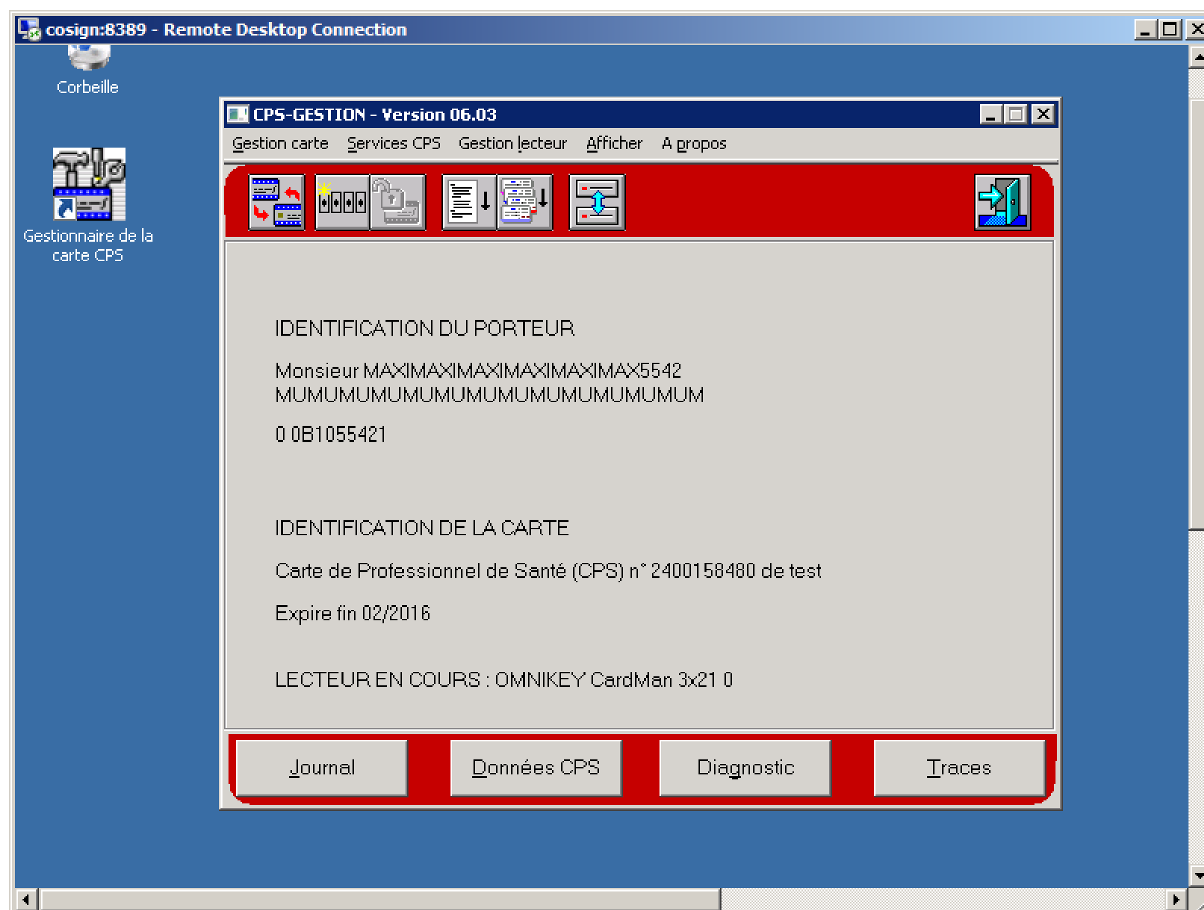


Figure 148 : Active Directory: Configuration: Bureau à distance et CPS Gestion après Smartcard logon

12.13 Paramétrage du Smartcard logon sur des nouveaux comptes AD

Le paramétrage démontré précédemment permet de configurer des comptes nouvellement créés pour le cas d'usage spécifique du Smartcard logon.

Le cas d'utilisation le plus fréquent concerne cependant l'ajout de la possibilité de faire du Smartcard logon à des comptes AD préexistants.

Cette section décrit le paramétrage et les développements nécessaires pour implémenter ce cas d'usage.

12.13.1 Script de déploiement des UPNs dans un active directory

La manière la plus simple de relier une carte CPS à un utilisateur stocké dans un annuaire Active Directory est d'éditer directement cet utilisateur dans l'Active Directory en lui attribuant l'UPN de la carte CPS correspondante, dans ses propriétés.

Néanmoins, dans les grosses structures contenant des centaines, voire des milliers d'utilisateurs déjà existants, il sera fastidieux de modifier manuellement chaque utilisateur.

On utilise alors, pour faciliter le déploiement, des scripts de modification de l'Active Directory, automatisés.

Les langages de scripts les plus courants sont :

- VBS (Visual Basic Scripting)
  - vivement déconseillé, sauf à disposer de compétences déjà bien établies sur cette technologie
- Windows PowerShell
  - Vivement conseillé

Ce sont des outils puissants de création de scripts d'administration.

Deux exemples de scripts VBS sont fournis ci-dessous.

Ils permettent l'ajout ou la modification de comptes utilisateurs dans un Active Directory.

La modification des utilisateurs se base sur une liste d'utilisateurs existants, reformatée dans un fichier texte dont la grammaire est fournie.

Ces scripts sont à adapter en fonction de l'architecture existante :

- utilisateurs stockés dans des OUs particuliers
- connexion à l'AD différente
- modification d'autres caractéristiques des utilisateurs
- etc…

Le script qui suit est un exemple de script VBS permettant la modification de l'UPN d'utilisateurs existants dans un annuaire Active Directory, à partir d'une liste d'utilisateurs/UPNs stockée dans un fichier texte (ici « **c:\users.txt** ») :

```
set Root = GetObject("LDAP://RootDSE")
DomainPath = Root.Get("DefaultNamingContext")
Set Domain = GetObject("LDAP://" & DomainPath)
wscript.echo DomainPath 'nom de domaine récupéré
' modification utilisateurs en masse
Const ForReading = 1
numError = 0
set fso = CreateObject("Scripting.FileSystemObject")
set usersTextFile = fso.OpenTextFile("C:\users.txt", ForReading, False) 'ouverture du fichier texte des utilisateurs
On error Resume next
While Not usersTextFile.atEndOfStream 'boucle sur le fichier texte
strRecord = usersTextFile.ReadLine ' Lecture d une ligne entiere
arrRecord = Split(strRecord, ";") ' decoupage avec caractere de separation ;
wscript.echo "utilisateur : " & arrRecord(0) & " - UPN: " & arrRecord(1)
Set objUser = GetObject("LDAP://localhost:389/CN=" & arrRecord(0) & ",CN=Users,"& DomainPath) ' connexion a l'objet USER
if (Err.Number <> 0) then
Err.Number = 0
wscript.echo "erreur : utilisateur introuvable: " & arrRecord(0)
numError = numError + 1
end if
objUser.Put "UserPrincipalName", arrRecord(1) '----- modification de l UPN
objUser.SetInfo 'validation de la modification
Wend
usersTextFile.close 'fermeture du fichier texte
wscript.echo "FIN script modification utilisateur OK : nombre d'erreurs : " & numError
```

Tableau 28 : Déploiement UPN : Exemple de script VBS permettant la modification de l'UPN d'utilisateurs existants dans un annuaire Active Directory

Le fichier **c:\users.txt** correspondant contiendrait des données organisées de cette manière:

```
user1;8.99700011141@carte-cps.fr
user2;8.99700011142@carte-cps.fr
user3;8.99700011143@carte-cps.fr
user4;8.99700011144@carte-cps.fr
user5;8.99700011145@carte-cps.fr
user6;8.99700011146@carte-cps.fr
user7;8.99700011147@carte-cps.fr
user8;8.99700011148@carte-cps.fr
```

Tableau 29: Déploiement UPN : Exemple de Fichier « users.txt »

Ci-après, un exemple de script VBS permettant la création d'utilisateurs en masse (ici 10), dans un annuaire Active Directory :

```
set Root = GetObject("LDAP://RootDSE")
DomainPath = Root.Get("DefaultNamingContext")
Set Domain = GetObject("LDAP://" & DomainPath)
wscript.echo DomainPath 'nom de domaine récupéré
Set objOU = GetObject("LDAP://localhost:389/CN=Users," & DomainPath)
for i =1 to 10 ' Ajout ici de 10 utilisateurs automatiquement
Set objUSER = objOU.Create("User", "cn=testUSERnum" & i)
objUser.Put "givenName", "test_givenName" &i
objUser.Put "sn", "test_surName"&i
objUser.Put "displayName", "test_DisplayName"&i
objUser.Put "SAMAccountName", "USER_test" & i
objUser.Put "UserPrincipalName", "UPNtest" & i & "@carte-cps.fr"
objUser.Put "mail", "test_mail@asipsante.fr"
objUser.Put "initials", "asip" & i
objUser.SetInfo
objUser.AccountDisabled = FALSE ' activation du compte
objUser.SetInfo
Next
wscript.echo "FIN script ajout utilisateur OK."
```

Tableau 30 : Déploiement UPN: Exemple de script VBS permettant la création d'utilisateurs dans un annuaire Active Directory

12.14 Paramétrage du Smartcard logon sur des comptes AD préexistants

12.14.1 Cas "1-to-1" : {un compte existant ; une carte}

Dans le cas bijectif {un compte existant ; une carte}, l'idée est de ramener à la déclaration de compte de :

Propriétés de : Carte6 Carte6. Carte6

Environnement | Sessions | Contrôle à distance
Profil des services Bureau à distance | Bureau virtuel personnel | COM+
Général | Adresse | Compte | Profil | Téléphones | Organisation | Membre de | Appel entrant

Nom d'ouverture de session de l'utilisateur :
Carte6 @eu.cosign
Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :
cosign\ Carte6
Horaires d'accès... Se connecter à...
Déverrouiller le compte
Options de compte :
L'utilisateur devra changer le mot de passe
L'utilisateur ne peut pas changer de mot de passe
Le mot de passe n'expire jamais
Enregistrer le mot de passe en utilisant un chiffrement réversible
Date d'expiration du compte
Jamais
Fin de : samedi 15 novembre 2014
OK Annuler Appliquer Aide

à:

Propriétés de : Carte6 Carte6. Carte6

Environnement | Sessions | Contrôle à distance
Profil des services Bureau à distance | Bureau virtuel personnel | COM+
Général | Adresse | Compte | Profil | Téléphones | Organisation | Membre de | Appel entrant

Nom d'ouverture de session de l'utilisateur :
0.0B1055413 @carte-cps.fr
Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :
cosign\ Carte6
Horaires d'accès... Se connecter à...
Déverrouiller le compte
Options de compte :
L'utilisateur devra changer le mot de passe
L'utilisateur ne peut pas changer de mot de passe
Le mot de passe n'expire jamais
Enregistrer le mot de passe en utilisant un chiffrement réversible
Date d'expiration du compte
Jamais
Fin de : samedi 15 novembre 2014
OK Annuler Appliquer Aide

Figure 149 : Paramétrage du Smartcard logon sur des comptes AD préexistants : cas {un compte existant ; une carte}

Dans ce cas, l'utilisateur peut se logger en Smartcard logon avec sa carte CPx (UPN 0.0B1055413@carte-cps.fr ici).

Il peut aussi se logger en login / mot de passe en utilisant dans ce cas:

- Login : COSIGN\Carte6 (à adapter)
- Mot de passe : son_mot_de_passe

Cette opération peut être automatisée.

12.14.2 Cas "n-to-m" : mappages de comptes existants sur des attributs de certificats X509 [Win2008R2]

Il est possible d'associer plusieurs cartes un utilisateur ou même 1 carte à plusieurs utilisateurs (ce dernier cas étant par ailleurs déconseillé).

Ce cas permet aussi de retrouver le cas particulier "1-to-1", sans éditer le nom d'ouverture de session utilisateur mais en perdant en ergonomie (voir ci-après).

Lancer la gestion d'utilisateur dans une MMS en choisissant les « Fonctionnalités avancées »

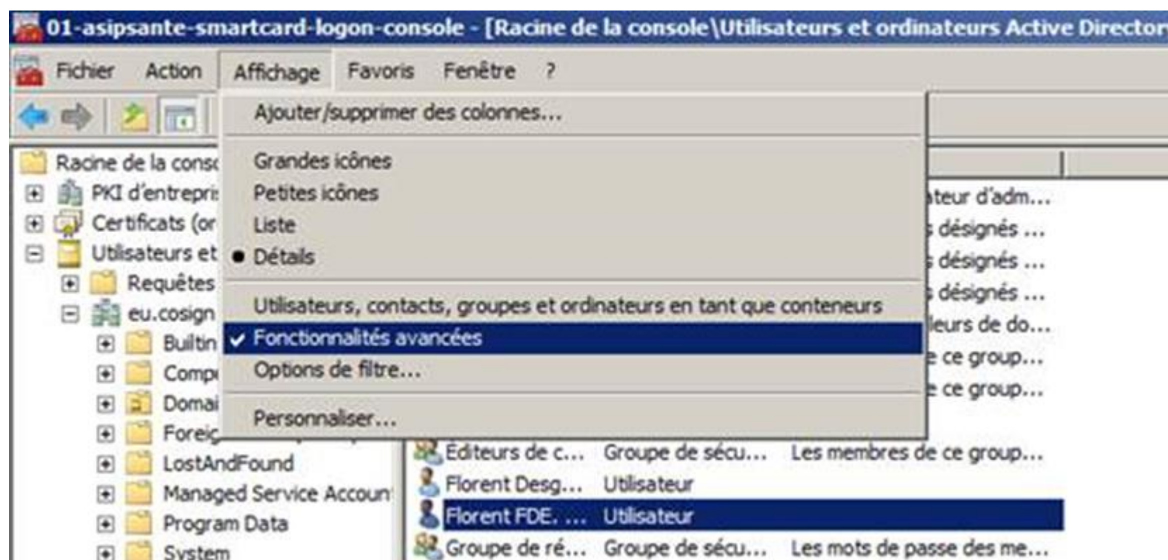


Figure 150 : Active Directory: Configuration du Smartcard logon pour utilisateurs existants

Clic-droit sur le « user » :

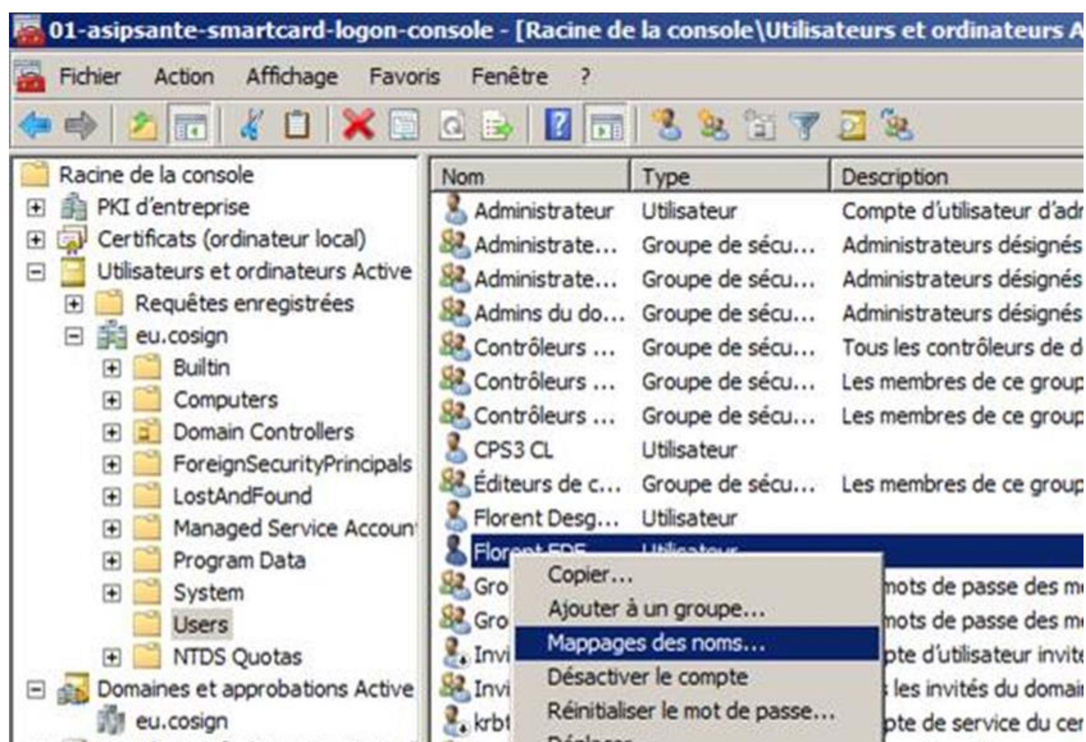


Figure 151 : Active Directory: Configuration du Smartcard logon pour utilisateurs existants

Choisir « Mappages des noms » :

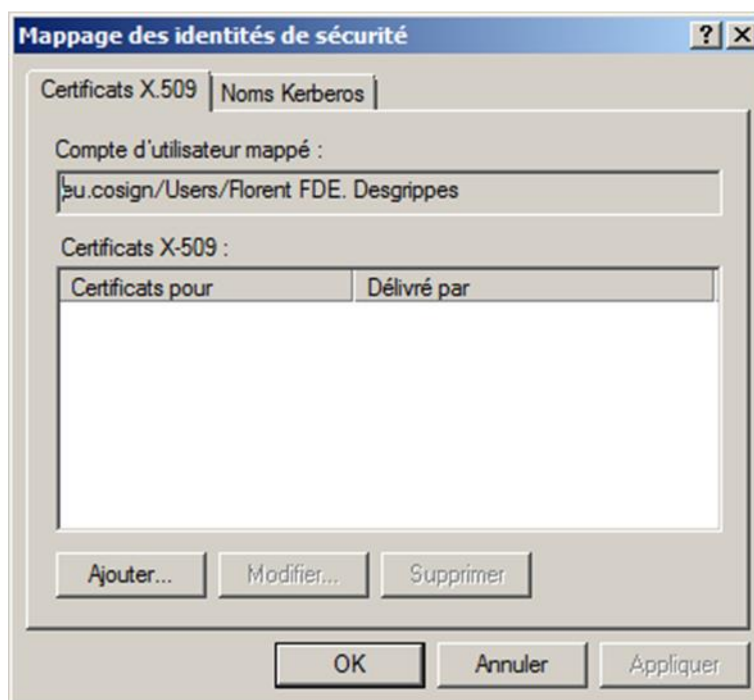


Figure 152 : Active Directory: Configuration du Smartcard logon pour utilisateurs existants

Ajouter le certificat carte :

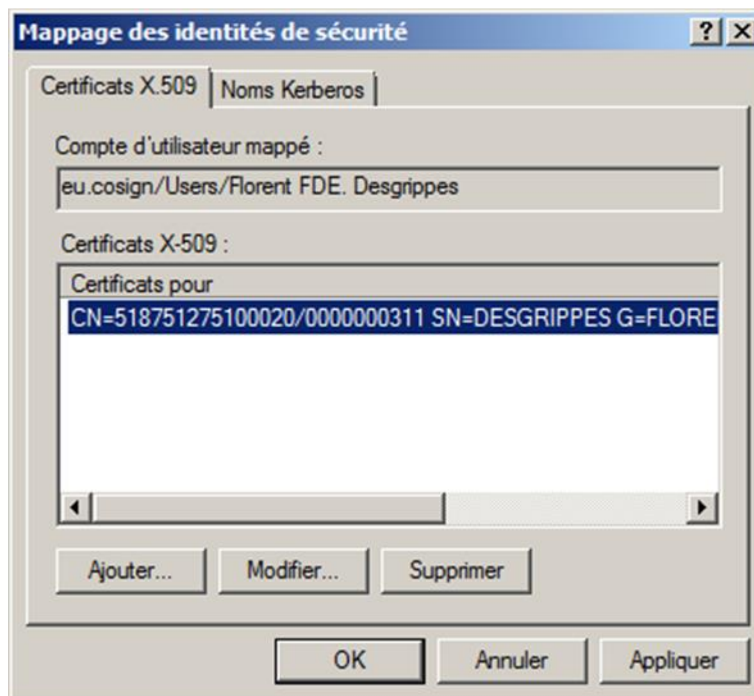


Figure 153 : Active Directory: Configuration du Smartcard logon pour utilisateurs existants

Cela correspond en fait à une alimentation des attributs de l'utilisateur dans l'AD :

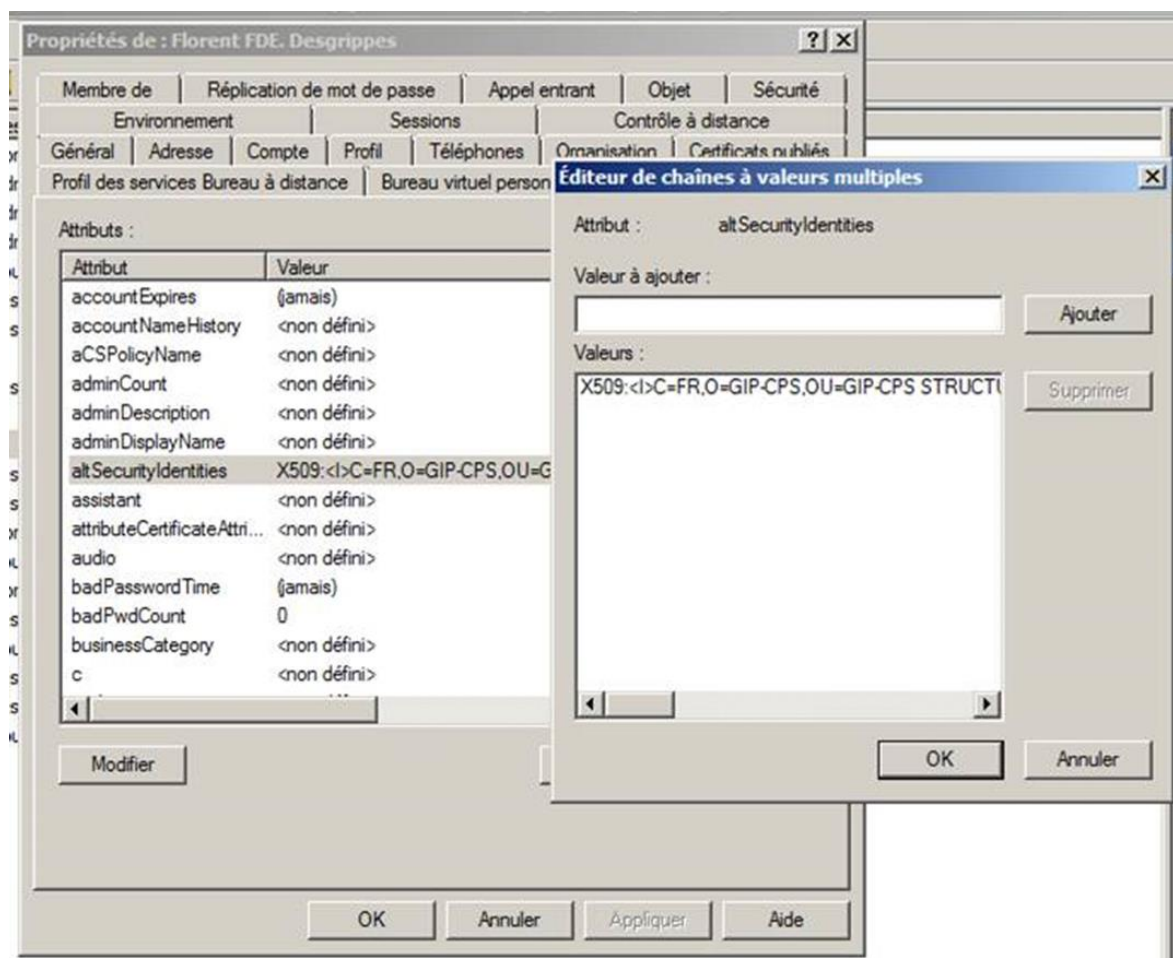


Figure 154 : Active Directory: Configuration du Smartcard logon pour utilisateurs existants

Cet enrôlement est automatisable sans qu'il soit nécessaire d'extraire tous les certificats d'authentification de tous les porteurs.

Le format choisi par défaut par Windows pour la chaine de caractère d'identification est :

X509:<I>issuer dn(dn de l'émetteur du certificat carte)<S>subject dn (dn du certificat de la carte)

L'ensemble des possibilités de mapping user / certificat étant :

Méthode	altSecurityIdentities
UPN	
Subject and Issuer fields	X509:<I>issuer dn(dn de l'émetteur du certificat carte)<S>subject dn (dn du certificat de la carte)
	X509:<I>C=FR,O=TEST,OU=TEST PROFESSIONNEL,CN=TEST CLASSE-1<S> C=FR,O=TEST,OU=Médecin,CN=00B1051552+SN=MAXIMAXIMAXIMAXIMAXIMAX5155+G=MUMUMUMUMUMUMUMUMUMUMUMUMUM
Subject DN	X509:<S>subject dn (dn du certificat de la carte)
	X509:<S> C=FR,O=TEST,OU=Médecin,CN=00B1051552+SN=MAXIMAXIMAXIMAXIMAXIMAX5155+G=MUMUMUMUMUMUMUMUMUMUMUMUMUM
Subject Key Identifier	X509:<SKI>subject key identifier (Identificateur de la clé du sujet)
	X509:<SKI>b8b585887bd28b0276a58ee878d9f8bfda85fa89
Issuer, and Serial Number	X509:<I>issuer dn(dn de l'émetteur du certificat carte)<SR>reverse(numéro de série (serial number))
	Serial number=4c 70 7d => 7d704c X509:<I>C=FR,O=TEST,OU=TEST PROFESSIONNEL,CN=TEST CLASSE-1<SR>7d704c
SHA1 Hash	X509:<SHA1-PUKEY>thumbprint (empreinte numérique)
	X509:<SHA1-PUKEY>2bbafed16923267e1a0d205557749691d7829103
RFC822 name	X509:<RFC822>adresse email précisée dans le SAN du certificat
	Méthode non disponible avec les certificats de l'IGC de Santé CPS2Ter actuellement en production (pas de champ email dans le SAN).

Tableau 31 : Liste des possibilités de mapping user / certificat pour l'authentification par certificat

12.14.3 Cas "n-to-m" : Désactivation de l'utilisation du subjectAltName (SAN)

Par contre, dans le cas du Smartcard logon (authentification par certificat venant d'une carte à puce), l'utilisateur va soumettre son certificat par l'intermédiaire des « couches carte à puce » de Windows qui va chercher, par défaut, à exploiter le subjectAltName (SAN) du certificat pour authentifier l'utilisateur : il faut donc désactiver l'usage du subjectAltName (SAN):

L'usage du subjectAltName (SAN) se désactive en appliquant les paramètres de base de registre suivants :

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kdc]
"UseSubjectAltName"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters]
"UseSubjectAltName"=dword:00000000
```

Tableau 32 : Désactivation de l'utilisation du SubjectAltName (SAN)

Cette désactivation doit être effectuée sur tous les KDC.

12.14.4 Cas "n-to-m" : Activation du « hint »

Il faut aussi modifier la GPO **Default Domain Policy** pour **activer** la politique :

« MMC -> Default Domain Policy -> Computer Configuration -> Administrative Templates -> Windows Components -> Smart Card -> Allow user name hint »
« MMC -> Default Domain Policy -> Configuration ordinateur -> Stratégies -> Modèles d'administration -> Carte à puce -> Autoriser l'indication du nom d'utilisateur »

Tableau 33 : Activation du « hint »

Afin que de permettre au KDC de retrouver le compte AD:

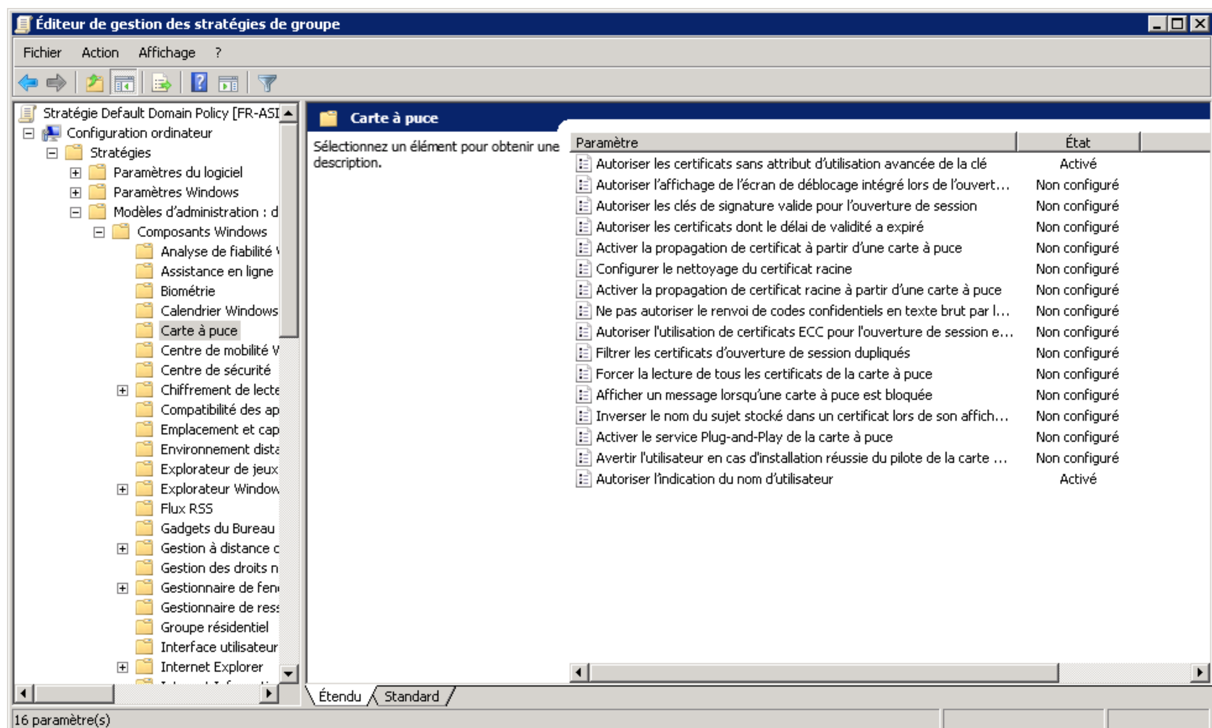


Figure 155 : Active Directory: Configuration du Smartcard logon pour utilisateurs existants : GPO « Allow user hint »

Les références pour ce cas d'usage sont :

#	Références
1	UseSubjectAltName and smartcard logon http://blogs.technet.com/b/instan/archive/2010/06/16/usesubjectaltname-and-smartcard-logon.aspx
2	Disable UPN mapping for SmartCard logon http://blogs.msdn.com/b/spatdsg/archive/2010/06/14/howto_3a00_-disable-upn-mapping-for-smartcard-logon.aspx
3	Map a user to a certificate via all the methods available in the altSecurityIdentities attribute http://blogs.msdn.com/b/spatdsg/archive/2010/06/18/howto-map-a-user-to-a-certificate-via-all-the-methods-available-in-the-altsecurityidentities-attribute.aspx

Tableau 34 : Active Directory: Configuration du Smartcard logon pour utilisateurs existants : Références

12.14.5 Cas "n-to-m" : Interface de logon et ergonomie

Les écrans de Winlogon sont alors les suivants :

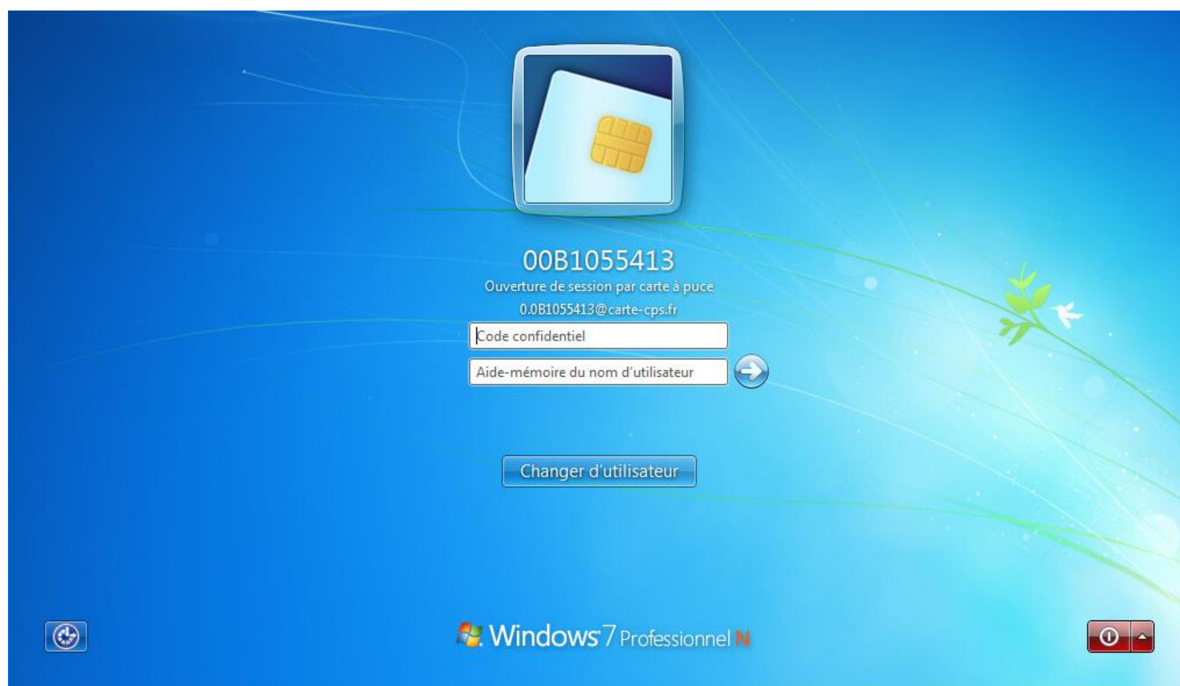


Figure 156 : Comptes existants : Ecran de Smartcard logon après lecture d'une carte

L'utilisateur saisit son code porteur et son compte dans le champ « hint » :



Figure 157 : Comptes existants : Saisie du code porteur et du « hint »

La session s'ouvre :



Figure 158 : Comptes existants : Ouverture de session Windows

L'ergonomie de ce scénario n'est pas aussi satisfaisante que celle associée à un compte pour lequel l'UPN du SAN est utilisé. Il est nécessaire de bien peser cet élément au moment de la définition du projet.

Tableau 35 : Comptes existants : Considération d'ergonomie en Smartcard logon sur compte préexistant

12.15 Configuration de la stratégie de détection d'arrachage de la carte

- Démarrer > Exécuter…> services.msc
- Localiser « Stratégie de retrait de la carte à puce » :

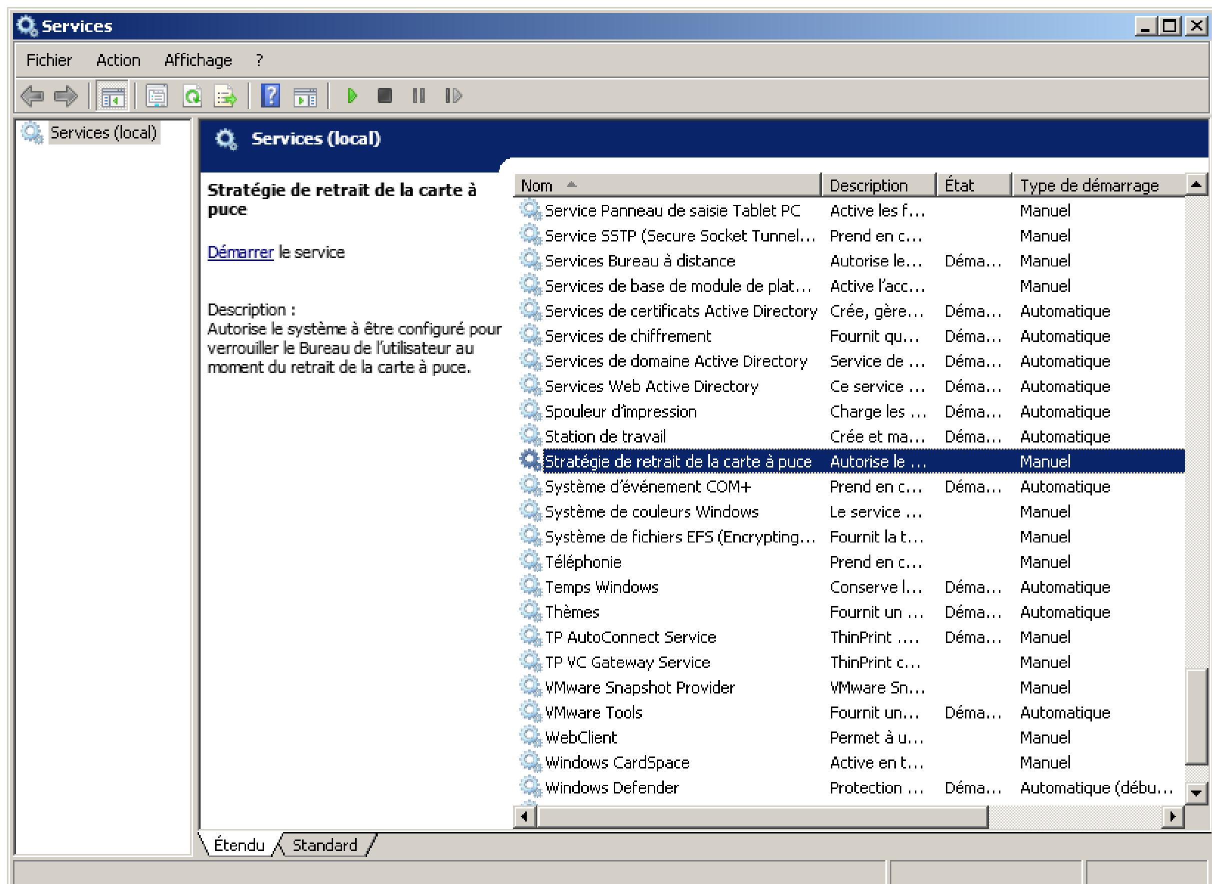


Figure 159 : Configuration de la Stratégie de retrait de la carte à puce (manuel)

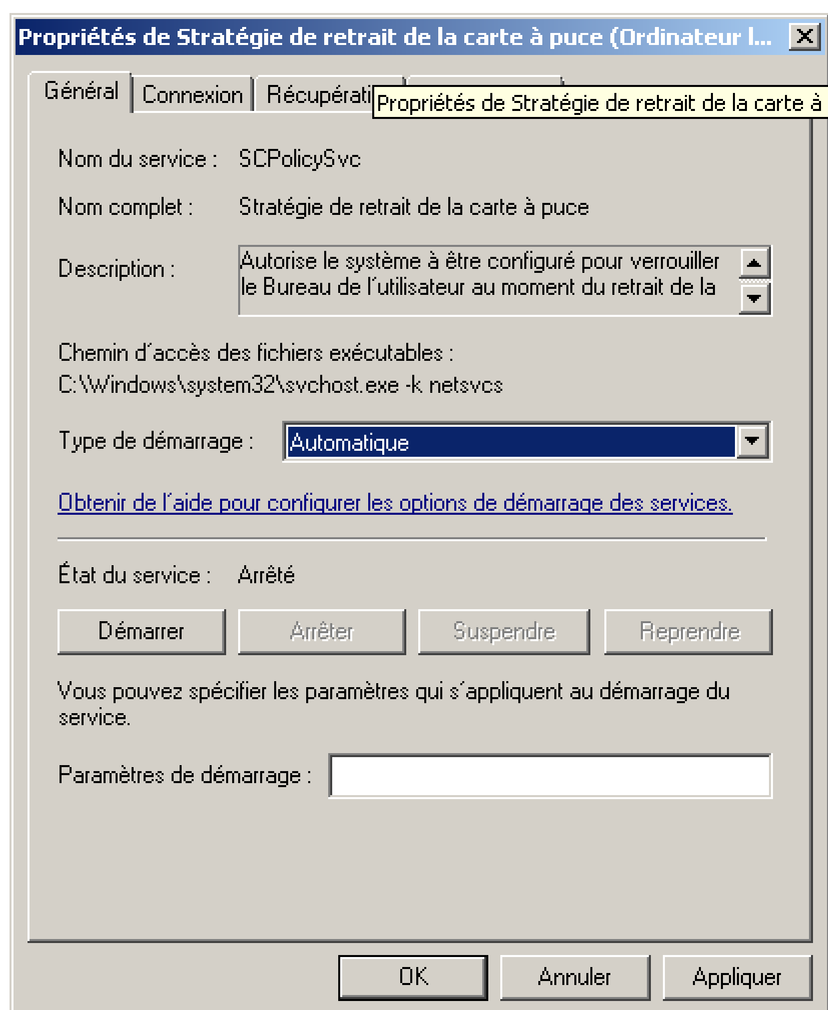


Figure 160 : Configuration de la Stratégie de retrait de la carte à puce (passage en automatique)

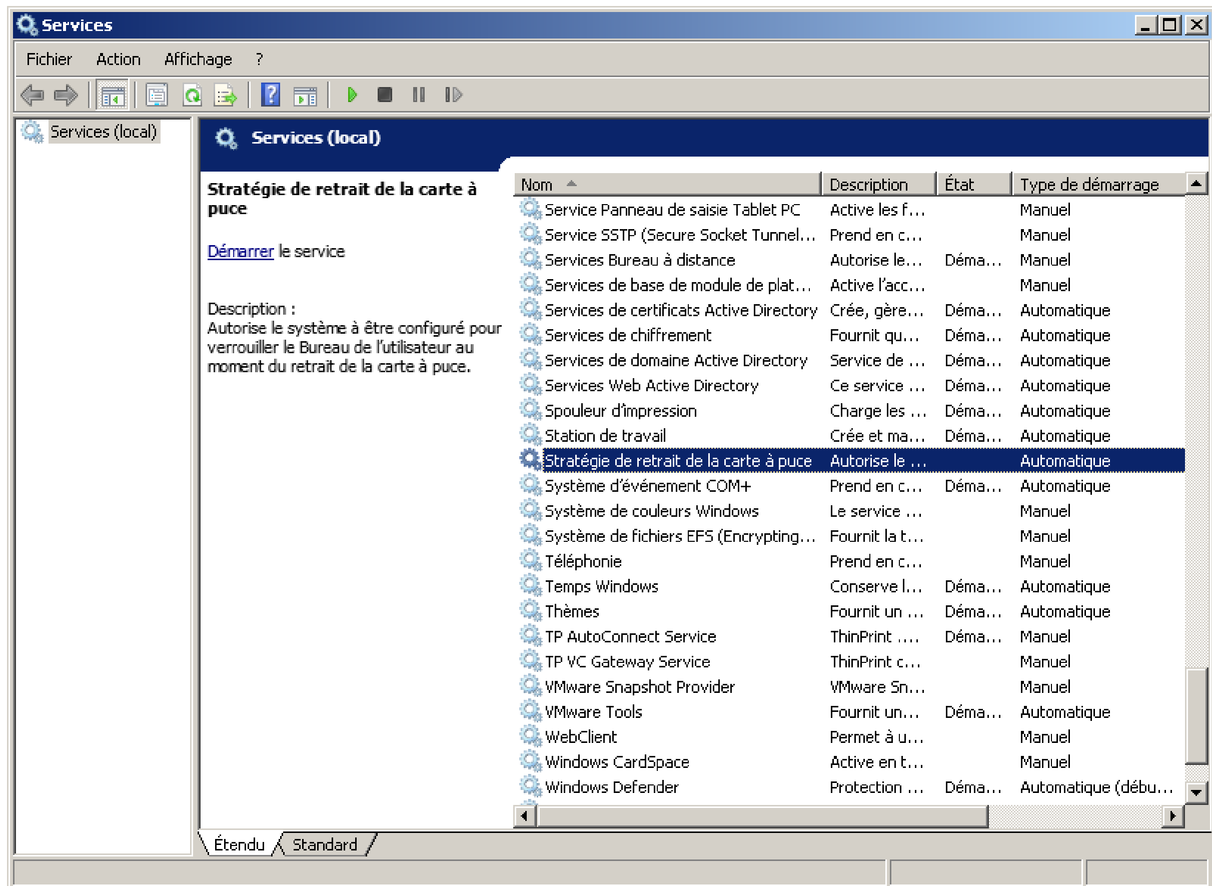


Figure 161 : Configuration de la Stratégie de retrait de la carte à puce (automatique)

12.16 Détails des certificats ASIP Santé

Abréviation	Local Machine	Rôle dans l'infrastructure	Fonction	Détails
LM Perso.	Local Machine	Domain Controller	Magasin de certificats	Personnel
LM Inter.	Local Machine	Domain Controller	Magasin de certificats	Intermédiaire
LM Root	Local Machine	Domain Controller	Magasin de certificats	Racine
NTAuth	Local Machine	Domain Controller	Active Directory	NTAuth
Strat. Ro.	Local Machine	Domain Controller	Stratégie de clé publique	Racine
Strat. Int.	Local Machine	Domain Controller	Stratégie de clé publique	Intermédiaire

Env.	Type	DN	IssuerDN	Fichier (rép. cer\cer\)	Thumbprint (SHA-1)	SubjectKeyIdentifier	AuthorityKeyIdentifier	LM Perso.	LM inter.	LM root	NTAuth	Strat. Ro.	Start. Int.	Check
Prod	Root	O=GIP-CPS, C=FR	O=GIP-CPS, C=FR	01-root-GIP-CPS.cer	8E4471D30842B54BC7E2582770009469ABD02CC7	E7A8FD8D3D091696AEFC7563279023795E5BD9B4		x		x	x	x		
Prod	Root	OU=ASIP-SANTE TECHNIQUE, O=ASIP-SANTE, C=FR	OU=ASIP-SANTE TECHNIQUE, O=ASIP-SANTE, C=FR	02-root-ASIPSANTE TECHNIQUE.cer	4AAA2092B960A4D9A8E6E917A6791A14A5E61F39	951EE95DC79A8E05E0AE7DE13D8F5D804D4C7861		x		x	x	x		
Prod	Root	OU=GIP-CPS ANONYME, O=GIP-CPS, C=FR	OU=GIP-CPS ANONYME, O=GIP-CPS, C=FR	03-root-GIP-CPS ANONYME.cer	552C001B751B326ACCCDFE9A6F1148ADCC687816	F1CFCF34D25A2F4B2B77D4B01F082DBF03C1FF77		x		x	x	x		

Env.	Type	DN	IssuerDN	Fichier (rép. cer\cer\)	Thumbprint (SHA-1)	SubjectKeyIdentifier	AuthorityKeyIdentifier	LM Perso.	LM inter.	LM root	NTAuth	Strat. Ro.	Start. Int.	Check
Prod	Root	OU=GIP-CPS PROFESSIONNEL, O=GIP-CPS, C=FR	OU=GIP-CPS PROFESSIONNEL, O=GIP-CPS, C=FR	04-root-GIP-CPS PROFESIONNEL.cer	9956634AD724F00A18C479E56463C6FB1C7A073D	CA2386BD652FBF507EB5B63A5D0C3356297597F3		x		x	x	x		
Prod	Root	OU=GIP-CPS STRUCTURE, O=GIP-CPS, C=FR	OU=GIP-CPS STRUCTURE, O=GIP-CPS, C=FR	05-root-GIP-CPS STRUCTURE.cer	514F46F3E278FBF6D8268286E19ADEE0CC443642	E7D8047AC370F8DC02E4A00B2CB275A59228FCBB		x		x	x	x		
Prod	Inter	CN=GIP-CPS CLASSE-0, OU=GIP-CPS ANONYME, O=GIP-CPS, C=FR	OU=GIP-CPS ANONYME, O=GIP-CPS, C=FR	06-inter-gip-cps-class0.cer	148D663D3F75DED92B5CB2608EEA182CCFB1862E	AA6638EFC10C44E1BA288B1AB0D4C272E7B49730	F1CFCF34D25A2F4B2B77D4B01F082DBF03C1FF77		x		x		x	
Prod	Inter	CN=GIP-CPS CLASSE-0, OU=GIP-CPS ANONYME, O=GIP-CPS, C=FR	OU=GIP-CPS ANONYME, O=GIP-CPS, C=FR	07-inter-gip-cps-class0.cer	052A8A966D4BF1E9832D717D98AD35C14EC9119C	FC3D7599995F2A1DDE244F7DF7AF30FCDE3C8CE3	F1CFCF34D25A2F4B2B77D4B01F082DBF03C1FF77		x		x		x	
Prod	Inter	CN=GIP-CPS CLASSE-1, OU=GIP-CPS PROFESSIONNEL, O=GIP-CPS, C=FR	OU=GIP-CPS PROFESSIONNEL, O=GIP-CPS, C=FR	08-inter-gip-cps-class1.cer	48630CFA410034E004A9BDB75D0CCB9DF8EBA4AC	3CBA21D0CD3D5E3EE335080A193ECBA9CBB24EBC	CA2386BD652FBF507EB5B63A5D0C3356297597F3		x		x		x	

Env.	Type	DN	IssuerDN	Fichier (rép. cer\cer\)	Thumbprint (SHA-1)	SubjectKeyIdentifier	AuthorityKeyIdentifier	LM Perso.	LM inter.	LM root	NTAuth	Strat. Ro.	Start. Int.	Check
Prod	Inter	CN=GIP-CPS CLASSE-1, OU=GIP-CPS PROFESSIONNEL, O=GIP-CPS, C=FR	OU=GIP-CPS PROFESSIONNEL, O=GIP-CPS, C=FR	09-inter-gip-cps-class1.cer	46934C7CDAD63C04B3FE76F5FFBF7512E55B8F7E	726C14AEAD8384AD2B174AC023959331DF256735	CA2386BD652FBF507EB5B63A5D0C3356297597F3		x		x		x	
Prod	Inter	CN=GIP-CPS CLASSE-2, OU=GIP-CPS STRUCTURE, O=GIP-CPS, C=FR	OU=GIP-CPS STRUCTURE, O=GIP-CPS, C=FR	10-inter-gip-cps-class2.cer	8A94BBBB12BD5567318FCF191B349B8FFD8A992D	F34F6B7F90A2A51F1F46A687AD8615B1010A62D6	E7D8047AC370F8DC02E4A00B2CB275A59228FCBB		x		x		x	
Prod	Inter	CN=GIP-CPS CLASSE-2, OU=GIP-CPS STRUCTURE, O=GIP-CPS, C=FR	OU=GIP-CPS STRUCTURE, O=GIP-CPS, C=FR	11-inter-gip-cps-class2.cer	3E85E5F32C4C2E6F2D82884228C515AE73A5C8D7	935920931D30024DD1BB2D2DD105BF1373A94D00	E7D8047AC370F8DC02E4A00B2CB275A59228FCBB		x		x		x	
Prod	Inter	CN=GIP-CPS CLASSE-3, OU=GIP-CPS STRUCTURE, O=GIP-CPS, C=FR	OU=GIP-CPS STRUCTURE, O=GIP-CPS, C=FR	12-inter-gip-cps-class3.cer	BA33690A8AC857D5E5514AC5FD817EE8CA1F7819	49025F3483F2E9655353FFCFBD8E638615008AA0	E7D8047AC370F8DC02E4A00B2CB275A59228FCBB		x		x		x	

Env.	Type	DN	IssuerDN	Fichier (rép. cer\cer\)	Thumbprint (SHA-1)	SubjectKeyIdentifier	AuthorityKeyIdentifier	LM Perso.	LM inter.	LM root	NTAuth	Strat. Ro.	Start. Int.	Check
Prod	Inter	CN=GIP-CPS CLASSE-3, OU=GIP-CPS STRUCTURE, O=GIP-CPS, C=FR	OU=GIP-CPS STRUCTURE, O=GIP-CPS, C=FR	13-inter-gip-cps-class3.cer	9F92B6CBF7FC61EBEA76F63ADD8D54C1AC2DDFB8	16E5E9F2E7246988DA3B7F2AF6690FC49BEFBE85	E7D8047AC370F8DC02E4A00B2CB275A59228FCBB		x		x		x	
Prod	Inter	O=GIP-CPS, C=FR	O=GIP-CPS, C=FR	14-inter-gip-cps.cer	4AC2FC4B4AD077669A9A6C4ACF8FA71810717407	ED5A0A4E712B0E5C4FA1E48B9162549675C73B18	E7A8FD8D3D091696AEFC7563279023795E5BD9B4		x		x		x	
Prod	Inter	OU=AC-CLASSE-4, O=GIP-CPS, C=FR	O=GIP-CPS, C=FR	15-inter-ac-class4.cer	3182462F180AE880B6F43FA040CEC025DC2F2042	25AF15AFC24AAE48D1CF241B14B8FC7D0F041FEB	E7A8FD8D3D091696AEFC7563279023795E5BD9B4		x		x		x	
Prod	Inter	OU=AC-CLASSE-5, O=GIP-CPS, C=FR	O=GIP-CPS, C=FR	16-inter-ac-class5.cer	5F3C2C90B974FE9FA8F9D2BDE11338C4D2681E37	A2CB0165BA5C4085F3FB071C3014C85EEF3C2A26	E7A8FD8D3D091696AEFC7563279023795E5BD9B4		x		x		x	
Prod	Inter	OU=AC-CLASSE-6, O=GIP-CPS, C=FR	O=GIP-CPS, C=FR	17-inter-ac-class6.cer	08C053B382E9D794FD7A9C44679B95E5C6B21B84	9691F5B5F398DF14B370E777A31B2F7E26B6FFB9	E7A8FD8D3D091696AEFC7563279023795E5BD9B4		x		x		x	
Prod	Inter	OU=GIP-CPS ANONYME, O=GIP-CPS, C=FR	OU=GIP-CPS ANONYME, O=GIP-CPS, C=FR	18-inter-gip-cps-anonyme.cer	BED257C7AC336AA2AC6DDE832B2EA3D2E10FD6EB	19ADD26C1AC9C7FC1AD8C4308563E57702F0D7E2	F1CFCF34D25A2F4B2B77D4B01F082DBF03C1FF77		x		x		x	
Prod	Inter	OU=GIP-CPS PROFESSIONNEL, O=GIP-CPS, C=FR	OU=GIP-CPS PROFESSIONNEL, O=GIP-CPS, C=FR	19-inter-gip-cps-professionnel.cer	307E5E5CB30966F05DF1670927A6154E91719EF3	C3692C6AC8592E8638779AEB1F055BE2F112EA92	CA2386BD652FBF507EB5B63A5D0C3356297597F3		x		x		x	

Env.	Type	DN	IssuerDN	Fichier (rép. cer\cer\)	Thumbprint (SHA-1)	SubjectKeyIdentifier	AuthorityKeyIdentifier	LM Perso.	LM inter.	LM root	NTAuth	Strat. Ro.	Start. Int.	Check
Prod	Inter	OU=GIP-CPS STRUCTURE, O=GIP-CPS, C=FR	OU=GIP-CPS STRUCTURE, O=GIP-CPS, C=FR	20-inter-gip-cps-structure.cer	D031C6132A5345BCBC52C499B89B87E40A077BFE	ACE6F2C855B2CE350304710C119F5070545D4F06	E7D8047AC370F8DC02E4A00B2CB275A59228FCBB		x		x		x	
Test	Root	O=GIP-CPS-TEST, C=FR	O=GIP-CPS-TEST, C=FR	21-root-GIP-CPS TEST.cer	717E472799B45FF755A97A0F2F2B30245C7FE379	AF3B167480F5D9547A21C738E625FA24FE34D504		x		x	x	x		
Test	Root	OU=TEST ANONYME, O=TEST, C=FR	OU=TEST ANONYME, O=TEST, C=FR	22-root-TEST ANONYME.cer	B8B9576489E0D294145C2016F61469E71CBF323F	97BF4F0C6226425292B9FA2673857014B55B243D		x		x	x	x		
Test	Root	OU=TEST PROFESSIONNEL, O=TEST, C=FR	OU=TEST PROFESSIONNEL, O=TEST, C=FR	23-root-TEST PROFESSIONNEL.cer	71E9AC03FCE3317707C7F5D5D429EA209ECA2305	75C14776C4AD282F67AA568B0322000C7AC38584		x		x	x	x		
Test	Root	OU=TEST STRUCTURE, O=TEST, C=FR	OU=TEST STRUCTURE, O=TEST, C=FR	24-root-TEST STRUCTURE.cer	90DA3E6D021FA378D55CEEEA3CE7B82CA7C8756B	54B7A98F06847DB7B79C35FB8FAE695D73D59375		x		x	x	x		
Test	Root	OU=TEST TECHNIQUE, O=TEST, C=FR	OU=TEST TECHNIQUE, O=TEST, C=FR	25-root-TEST TECHNIQUE.cer	42111D850BB4E3B4D30A920ACCB6D64BD9CA3F98	26ECC1EBBD3B9CCEAFF32FED04200D698593223D		x		x	x	x		
Test	Inter	CN=TEST CLASSE-0, OU=TEST ANONYME, O=TEST, C=FR	OU=TEST ANONYME, O=TEST, C=FR	26-inter-test-class0.cer	D367C327413DAEA682681C388C1C8DE3560BD841	4DB168E2C11E74F9FE368173340687E6D940F5B0	97BF4F0C6226425292B9FA2673857014B55B243D		x		x		x	

Env.	Type	DN	IssuerDN	Fichier (rép. cer\cer\)	Thumbprint (SHA-1)	SubjectKeyIdentifier	AuthorityKeyIdentifier	LM Perso.	LM inter.	LM root	NTAuth	Strat. Ro.	Start. Int.	Check
Test	Inter	CN=TEST CLASSE-0, OU=TEST ANONYME, O=TEST, C=FR	OU=TEST ANONYME, O=TEST, C=FR	27-inter-test-class0.cer	4443FC0599A80C3A61C416A9CD174BB9D42C61BF	898C2D753B73969C3BA1B1599868EDC1999E92EE	97BF4F0C6226425292B9FA2673857014B55B243D		x		x		x	
Test	Inter	CN=TEST CLASSE-1, OU=TEST PROFESSIONNEL, O=TEST, C=FR	OU=TEST PROFESSIONNEL, O=TEST, C=FR	28-inter-test-class1.cer	933D2D2BD62FFFD0CCE7FA092C0D34C3B64E69E7	0A26371072F587FCA7A0C4713D77F0BB235FEE4A	75C14776C4AD282F67AA568B0322000C7AC38584		x		x		x	
Test	Inter	CN=TEST CLASSE-1, OU=TEST PROFESSIONNEL, O=TEST, C=FR	OU=TEST PROFESSIONNEL, O=TEST, C=FR	29-inter-test-class1.cer	2438CFC8F2756CBB26850273F7A0E47C57B2233E	76103543B48B7F8C6E00B792A69082B3C14BD2EA	75C14776C4AD282F67AA568B0322000C7AC38584		x		x		x	
Test	Inter	CN=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR	OU=TEST STRUCTURE, O=TEST, C=FR	30-inter-test-class2.cer	B027E02F33F0DC12847CDE8B0BC0AC5B767E0473	DB39068C884F434D60505B3996737CD3A2DE5694	54B7A98F06847DB7B79C35FB8FAE695D73D59375		x		x		x	
Test	Inter	CN=TEST CLASSE-2, OU=TEST STRUCTURE, O=TEST, C=FR	OU=TEST STRUCTURE, O=TEST, C=FR	31-inter-test-class2.cer	54DFEE1AC4CD8D5ACF32F7AE121EF26A338FF13D	44721289C272779BDB0A3B8F4A32AE4E2CAF5876	54B7A98F06847DB7B79C35FB8FAE695D73D59375		x		x		x	

Env.	Type	DN	IssuerDN	Fichier (rép. cer\cer\)	Thumbprint (SHA-1)	SubjectKeyIdentifier	AuthorityKeyIdentifier	LM Perso.	LM inter.	LM root	NTAuth	Strat. Ro.	Start. Int.	Check
Test	Inter	CN=TEST CLASSE-3, OU=TEST STRUCTURE, O=TEST, C=FR	OU=TEST STRUCTURE, O=TEST, C=FR	32-inter-test-class3.cer	874F4F184DA9F896FADE58AADE1185467E63834A	6E721567491689E5F0DDD211D4701FEC6B55DB6A	54B7A98F06847DB7B79C35FB8FAE695D73D59375		x		x		x	
Test	Inter	CN=TEST CLASSE-3, OU=TEST STRUCTURE, O=TEST, C=FR	OU=TEST STRUCTURE, O=TEST, C=FR	33-inter-test-class3.cer	2BEB8461F6F2FEC5EE95872FCC52B9E736125CB1	06EEE31E10446ED72CD4A312D4427F289A5B94EF	54B7A98F06847DB7B79C35FB8FAE695D73D59375		x		x		x	
Test	Inter	O=GIP-CPS-TEST, C=FR	O=GIP-CPS-TEST, C=FR	34-inter-gip-cps-test.cer	5ED0889BCEAE671A4A368AB405E2B25431AC20D2	E1FA17F81423C5DE9F7B4956A2E542986CE44A2F	AF3B167480F5D9547A21C738E625FA24FE34D504		x		x		x	
Test	Inter	OU=AC-CLASSE-4-TEST, O=GIP-CPS-TEST, C=FR	O=GIP-CPS-TEST, C=FR	35-inter-ac-class4-test.cer	01ED444C889EF19F375EEB6D87137A84CF83BEB9	C256EFEF20F25917BC406C59B3CCF89B93BB681A	AF3B167480F5D9547A21C738E625FA24FE34D504		x		x		x	
Test	Inter	OU=AC-CLASSE-5-TEST, O=GIP-CPS-TEST, C=FR	O=GIP-CPS-TEST, C=FR	36-inter-ac-class5-test.cer	D202CB693A9668A50E28C967947AE7B84FE1C3EB	90DA136A53A6487AD32680936E708B93D2DEEC94	AF3B167480F5D9547A21C738E625FA24FE34D504		x		x		x	
Test	Inter	OU=AC-CLASSE-6-TEST, O=GIP-CPS, C=FR	O=GIP-CPS-TEST, C=FR	37-inter-ac-class6-test.cer	1235CB411691D50293DCA42AFA7297B934E10EB6	9805991A5C4935AABF7733FEEAB542C9B7A9D647	AF3B167480F5D9547A21C738E625FA24FE34D504		x		x		x	
Test	Inter	OU=TEST ANONYME, O=TEST, C=FR	OU=TEST ANONYME, O=TEST, C=FR	38-inter-test-anonyme.cer	EA2953E1AFCD8D7174508D211DD784ACB3F8CCDE	5B0EC162BE14E88F8727F96BBD84AC08F5FC7952	97BF4F0C6226425292B9FA2673857014B55B243D		x		x		x	

Env.	Type	DN	IssuerDN	Fichier (rép. cer\cer\)	Thumbprint (SHA-1)	SubjectKeyIdentifier	AuthorityKeyIdentifier	LM Perso.	LM inter.	LM root	NTAuth	Strat. Ro.	Start. Int.	Check
Test	Inter	OU=TEST PROFESSIONNEL, O=TEST, C=FR	OU=TEST PROFESSIONNEL, O=TEST, C=FR	39-inter-test-professionnel.cer	D7E070C9C5D645958317E023C855DC48FDB49F0C	254BDD0F8A5D08B05BBA312076A00255C08A0183	75C14776C4AD282F67AA568B0322000C7AC38584		x		x		x	
Test	Inter	OU=TEST STRUCTURE, O=TEST, C=FR	OU=TEST STRUCTURE, O=TEST, C=FR	40-inter-test-structure.cer	BD5976486680623C98B15F64C2884E2654E54446	9DAA04AFF9307FE3719DE1FFA62F0C8A242C05B8	54B7A98F06847DB7B79C35FB8FAE695D73D59375		x		x		x	
Prod	PKI Microsoft			%USERPROFILE%\Desktop**ad-cs-rootca.cer**				x	x	x	x	x		
Prod	PKI Microsoft			%USERPROFILE%\Desktop**ad-dc-rootca.cer**				x						
Prod	PKI Microsoft			%USERPROFILE%\Desktop**rd-rootca.cer**				x						

Env.	Type	DN	IssuerDN	Fichier (rép. cer\cer\)	Thumbprint (SHA-1)	SubjectKeyIdentifier	AuthorityKeyIdentifier	LM Perso.	LM inter.	LM root	NTAuth	Strat. Ro.	Start. Int.	Check
PFC NG	Root	CN=AC RACINE IGC-SANTE FORT, OU=IGC-SANTE, OU=0002 187512751, O=ASIP-SANTE, C=FR	CN=AC RACINE IGC-SANTE FORT, OU=IGC-SANTE, OU=0002 187512751, O=ASIP-SANTE, C=FR		BBE751C8B107ACD29F7D12E0FCDD717E00138764	38430511002EE752C3E8974674F8A4FB9CDCE5EE	38430511002EE752C3E8974674F8A4FB9CDCE5EE	x		x	x	x		
PFC NG	Root	CN=AC RACINE IGC-SANTE STANDARD, OU=IGC-SANTE, OU=0002 187512751, O=ASIP-SANTE, C=FR	CN=AC RACINE IGC-SANTE STANDARD, OU=IGC-SANTE, OU=0002 187512751, O=ASIP-SANTE, C=FR		B6BA1D6D5224BCEDA95A67F6F37B86896EDD0006	C0AC89F12470D52BE2D5D4B48405C0810572539B	C0AC89F12470D52BE2D5D4B48405C0810572539B	x		x	x	x		

Env.	Type	DN	IssuerDN	Fichier (rép. cer\cer\)	Thumbprint (SHA-1)	SubjectKeyIdentifier	AuthorityKeyIdentifier	LM Perso.	LM inter.	LM root	NTAuth	Strat. Ro.	Start. Int.	Check
PFC NG	Root	CN=AC RACINE IGC-SANTE ELEMENTAIRE, OU=IGC-SANTE, OU=0002 187512751, O=ASIP-SANTE, C=FR	CN=AC RACINE IGC-SANTE ELEMENTAIRE, OU=IGC-SANTE, OU=0002 187512751, O=ASIP-SANTE, C=FR		4B23D44DC5CBDA230FC052DFF52407EDAF373C69	8C6FEAD58B82FAF9BE87DC730E27150747C49E2F	8C6FEAD58B82FAF9BE87DC730E27150747C49E2F	x		x	x	x		
PFC NG	Inter	CN=AC IGC-SANTE FORT ORGANISATIONS, OU=IGC-SANTE, OU=0002 187512751, O=ASIP-SANTE, C=FR	CN=AC RACINE IGC-SANTE FORT, OU=IGC-SANTE, OU=0002 187512751, O=ASIP-SANTE, C=FR		7C3AF35B76FE34699FBC72C6A340BC7F1AC4D854	EDE618D2E0FE7345CBF8242F566BA606E20F7331	38430511002EE752C3E8974674F8A4FB9CDCE5EE		x		x		x	

Env.	Type	DN	IssuerDN	Fichier (rép. cer\cer\)	Thumbprint (SHA-1)	SubjectKeyIdentifier	AuthorityKeyIdentifier	LM Perso.	LM inter.	LM root	NTAuth	Strat. Ro.	Start. Int.	Check
PFC NG	Inter	CN=AC IGC-SANTE FORT PERSONNES, OU=IGC-SANTE, OU=0002 187512751, O=ASIP-SANTE, C=FR	CN=AC RACINE IGC-SANTE FORT, OU=IGC-SANTE, OU=0002 187512751, O=ASIP-SANTE, C=FR		AA6131E760B95622C0F4C2AA9D985002C21F3A0C	800F918821797D5555C65D6DD5938D6ADE5C2AA6	38430511002EE752C3E8974674F8A4FB9CDCE5EE		x		x		x	
PFC NG	Inter	CN=AC IGC-SANTE STANDARD ORGANISATIONS, OU=IGC-SANTE, OU=0002 187512751, O=ASIP-SANTE, C=FR	CN=AC RACINE IGC-SANTE STANDARD, OU=IGC-SANTE, OU=0002 187512751, O=ASIP-SANTE, C=FR		EA8752036E115EE8AA1653672289074A24B23994	66B62D3DB8FC1E1A1349688284587324C4ACE5A0	C0AC89F12470D52BE2D5D4B48405C0810572539B		x		x		x	

Env.	Type	DN	IssuerDN	Fichier (rép. cer\cer\)	Thumbprint (SHA-1)	SubjectKeyIdentifier	AuthorityKeyIdentifier	LM Perso.	LM inter.	LM root	NTAuth	Strat. Ro.	Start. Int.	Check
PFC NG	Inter	CN=AC IGC-SANTE STANDARD PERSONNES, OU=IGC-SANTE, OU=0002 187512751, O=ASIP-SANTE, C=FR	CN=AC RACINE IGC-SANTE STANDARD, OU=IGC-SANTE, OU=0002 187512751, O=ASIP-SANTE, C=FR		E0D6E1D8481FED62C65C53ED9DFCDA949C3D1D81	19F276D58D7A17CA829BE97B5AEF3F05A690D4F3	C0AC89F12470D52BE2D5D4B48405C0810572539B		x		x		x	
PFC NG	Inter	CN=AC IGC-SANTE ELEMENTAIRE ORGANISATIONS, OU=IGC-SANTE, OU=0002 187512751, O=ASIP-SANTE, C=FR	CN=AC RACINE IGC-SANTE ELEMENTAIRE, OU=IGC-SANTE, OU=0002 187512751, O=ASIP-SANTE, C=FR		2CBFA991750AF778348B3156C21609A1AB45A848	D7FBFADCD5027FE7C153864D4BE8A44A1E0BBB63	8C6FEAD58B82FAF9BE87DC730E27150747C49E2F		x		x		x	

Env.	Type	DN	IssuerDN	Fichier (rép. cer\cer\)	Thumbprint (SHA-1)	SubjectKeyIdentifier	AuthorityKeyIdentifier	LM Perso.	LM inter.	LM root	NTAuth	Strat. Ro.	Start. Int.	Check
PFC NG	Inter	CN=AC IGC-SANTE ELEMENTAIRE PERSONNES, OU=IGC-SANTE, OU=0002 187512751, O=ASIP-SANTE, C=FR	CN=AC RACINE IGC-SANTE ELEMENTAIRE, OU=IGC-SANTE, OU=0002 187512751, O=ASIP-SANTE, C=FR		86A0DE3D866E2DB5095F6785A57FD5CC53B2F049	CEAF9B1C194A6B53A7A8C9D81FDB6114CD07F22E	8C6FEAD58B82FAF9BE87DC730E27150747C49E2F		x		x		x	

Tableau 36 : Liste de certificats

12.17 Debugging

12.17.1 Traces Cryptolib CPS

Gestion des traces Cryptolib CPS	
Activation en fusionnant le fichier	**%ProgramFiles%\santesocial\CPS\activation_traces.reg**
Traces générées dans le répertoire	**%ALLUSERSPROFILE%\santesocial\CPS\log**
Désactivation en fusionnant le fichier	**%ProgramFiles%\santesocial\CPS\desactivation_traces.reg**

Tableau 37 : Activation des traces Kerberos via la base de registre

12.17.2 Traces Kerberos

2 méthodes sont disponibles :

12.17.2.1 Via la base de registre

12.17.2.1.1 Activation

Les traces Kerberos s'activent en fusionnant les paramètres suivants en base de registre:

Activation des traces Kerberos via la base de registre	
En modifiant les clés suivantes :	*[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0]* *"NtLmInfoLevel"=dword:c0015003* *[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos]* *"LogToFile"=dword:00000001* *[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos\Parameters]* *"LogToFile"=dword:00000001* *[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos\Parameters]* *"KerbDebugLevel"=dword:c0000043* *[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Kdc]* *"KdcDebugLevel"=dword:c0000803*
En fusionnant le fichier suivant :	**log\kerberos-reg\debug-smartcard-logon-kerberos-activate.reg**

Tableau 38 : Activation des traces Kerberos via la base de registre

12.17.2.1.2Génération

Emplacement des traces Kerberos via la base de registre	
Répertoires suivants:	*%systemroot%\system32\lsass.log* *%systemroot%\tracing\msv1_0* *%systemroot%\tracing\kerberos* *%systemroot%\tracing\kdcsvc*

Tableau 39 : Emplacement des traces Kerberos après activation via la base de registre

12.17.2.1.3Désactivation

Les traces Kerberos se désactivent en fusionnant les paramètres suivants en base de registre:

Désactivation des traces Kerberos via la base de registre	
En modifiant les clés suivantes :	*[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0]* *"NtLmInfoLevel"=-* *[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos]* *"LogLevel"=-* *[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos]* *"LogToFile"=-* *[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos]* *"KerbDebugLevel"=-* *[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos\Parameters]* *"LogLevel"=-* *[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos\Parameters]* *"LogToFile"=-* *[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos\Parameters]* *"KerbDebugLevel"=-* *[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Kdc]* *"KdcDebugLevel"=-*
En fusionnant le fichier suivant :	**log\kerberos-reg\debug-smartcard-logon-kerberos-deactivate.reg**

Tableau 40 : Désactivation des traces Kerberos activées via la base de registre

12.17.2.2 Via Tracelog

Tracelog.exe est un outil Microsoft fourni avec Visual Studio ou avec le WDK (fourni dans le répertoire **bin** du Kit ASIP Santé Smartcard logon).

12.17.2.2.1 Activation

Activation des traces Kerberos via Tracelog	
En utilisant les appels:	*tracelog.exe -kd -rt -start ntlm -guid #5BBB6C18-AA45-49b1-A15F-085F7ED0AA90 -f .\ntlm.etl -flags 0x15003 -ft 1* *tracelog.exe -kd -rt -start kerb -guid #6B510852-3583-4e2d-AFFE-A67F9F223438 -f .\kerb.etl -flags 0x43 -ft 1* *tracelog.exe -kd -rt -start kdc -guid #1BBA8B19-7F31-43c0-9643-6E911F79A06B -f .\kdc.etl -flags 0x803 –ft 1*
En fusionnant le fichier de commande:	**log\kerberos-tracelog\02-asipsante-smartcard-logon-kerberos-tracelog.cmd start**

Tableau 41 : Activation des traces Kerberos via Tracelog

12.17.2.2.2 Génération

Emplacement des traces Kerberos via Tracelog	
Fichiers suivants:	*.\ntlm.etl* *.\kerb.etl* *.\kdc.etl*

Tableau 42 : Emplacement des traces Kerberos après activation via Tracelog

12.17.2.2.3 Désactivation

Activation des traces Kerberos via Tracelog	
En utilisant les appels:	*tracelog.exe -stop ntlm* *tracelog.exe -stop kerb* *tracelog.exe -stop kdc*
En fusionnant le fichier de commande:	**log\kerberos-tracelog\02-asipsante-smartcard-logon-kerberos-tracelog.cmd stop**

Tableau 43 : Désactivation des traces Kerberos activées via Tracelog

Attention :

- supprimer ou protéger les fichiers d'activation/désactivation de traces des machines de productions
- désactiver les traces avant de (re)passer en production (pénalisant pour les performances)

12.18 Points d’attention et contournements

12.18.1 Limitations

En date de juillet 2013 :

ID	Ticket(s)	OS	Archi	Limitation	Alternative	Statut Problème	Statut Alternative
AT_0010				**Env. TSE :** Les clients RDP installés avec les Cryptolib CPS « GALSS » 5.0.4 ou 5.0.6 ne fonctionnent pas en Smartcard Logon.	Installer les Cryptolib CPS v5.0.8 sur le poste client (cf. Annexe 6, installation du poste client), x64 sur les OS x64, x32 sur les OS x32	Confirmé	Confirmé
AT_0020	0001075			**Env. TSE :** Les serveurs RDP installés avec Cryptolib CPS v5.0.6 ne permettent pas de rouvrir une session après qu’une première session ait été ouverte préalablement.	Installer les Cryptolib CPS v5.0.8 côté serveur.	Confirmé	Confirmé

ID	Ticket(s)	OS	Archi	Limitation	Alternative	Statut Problème	Statut Alternative
AT_0030	0001074			**Env. TSE :** Sur une session verrouillée, l'introduction d'un mauvais code porteur déverrouille la session.	Installer les Cryptolib CPS v5.0.8 côté client et serveur.	Confirmé	Confirmé
AT_0040	0001071 0001073			**Env. TSE :** Lors d'une ouverture de session, le login reste bloqué sur « lecture de la carte à puce » si on retire la carte juste après son insertion.	Vérifier le comportement lorsque la GPO de propagation du certificat est désactivée.	Non reproduit	

ID	Ticket(s)	OS	Archi	Limitation	Alternative	Statut Problème	Statut Alternative
AT_0050	0001071 0001073			**Env. TSE :** Le service de propagation de certificat se bloque sur on retire la carte lors d'une lecture avec les Cryptolib CPS.	Vérifier le comportement lorsque la GPO de propagation du certificat est désactivée : **le CCM assure la propagation des certificats. Contrairement au Service de propagation MS, il assure le retrait des certificats du magasin lors du retrait carte.**	Non reproduit	
AT_0060	0001071 0001073			**Env. TSE :** L'ouverture de session reste bloquée sur « Bienvenue » lors d'authentification simultanées.		Non reproduit	

ID	Ticket(s)	OS	Archi	Limitation	Alternative	Statut Problème	Statut Alternative
AT_0070	0001075			**Env. TSE :** L'ouverture de session signale des erreurs.	Installer les Cryptolib CPS v5.0.8 sur le poste client (cf. Annexe 6, installation du poste client).	Confirmé	Confirmé

ID	Ticket(s)	OS	Archi	Limitation	Alternative	Statut Problème	Statut Alternative
AT_0080				**Env. TSE :** Il n’est pas possible d’ouvrir une session lorsque l’option SSL du service NLA (Network Level Authentication) SSL est activée. Cf. 6.5 « Installation d’un rôle Terminal Server »		**Non reproduit** 20130731 : Cette fonctionnalité est nouvelle dans W2008R2 (noyaux Vista+ et RDP 6.0), n’a pas encore été testée et n’est pas encore supportée.	

ID	Ticket(s)	OS	Archi	Limitation	Alternative	Statut Problème	Statut Alternative
AT_0090	0001075			**Env. TSE :** Une fenêtre d’erreur Microsoft Visual C++ apparait aléatoirement	Installer les Cryptolib CPS v5.0.8 côté client et serveur.	Confirmé	Confirmé

ID	Ticket(s)	OS	Archi	Limitation	Alternative	Statut Problème	Statut Alternative
AT_0100	0001047			**Env. Citrix** : http://support.citrix.com/article/CTX136248 http://support.citrix.com/article/CTX136922 cf. **[4]** ASIP-PTS-PSCE_Manuel-Installation-utilisation-Cryptolib-CPS_20140224_v5.0.2.pdf		Clos	
AT_0110				**Env. TSE :**Les utilisateurs ne peuvent pas utiliser une carte à puce pour se connecter à une session de Services Terminal Server sur un ordinateur qui exécute Windows Server 2008	Installer W2008R2 SP1 ou le KB958596 http://support.microsoft.com/kb/958596/en	Clos	
AT_0120				Available Updates for Remote Desktop Services (Terminal Services) on Windows Server 2008 R2 SP1	http://support.microsoft.com/?id=2601888 http://support.microsoft.com/kb/2521923	Clos	
AT_0130	0001097			La sélection automatique des certificats carte en Smartcard logon ne marche pas lorsque 2 cartes sont présentes sur le poste client. Il n'est pas possible d'ouvrir 2 sessions TSE automatiquement en parallèle avec 2 cartes depuis un même poste client. Les 2 sessions s'ouvrent sir la sélection est explicitée par l'utilisateur.	http://blogs.technet.com/b/instan/archive/2011/01/27/automatic-logon-to-rds-using-smartcards-with-multiple-certificates-with-or-without-ts-gateway.aspx	Clos	Clos

Tableau 44 : Points d'attention

12.18.2 Contournements

12.18.2.1 AT_0030 - Désactivation du verrouillage de session

Le minimum consiste à positionner cette valeur en base de registre:

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]

"DisableLockWorkstation"=dword:00000001

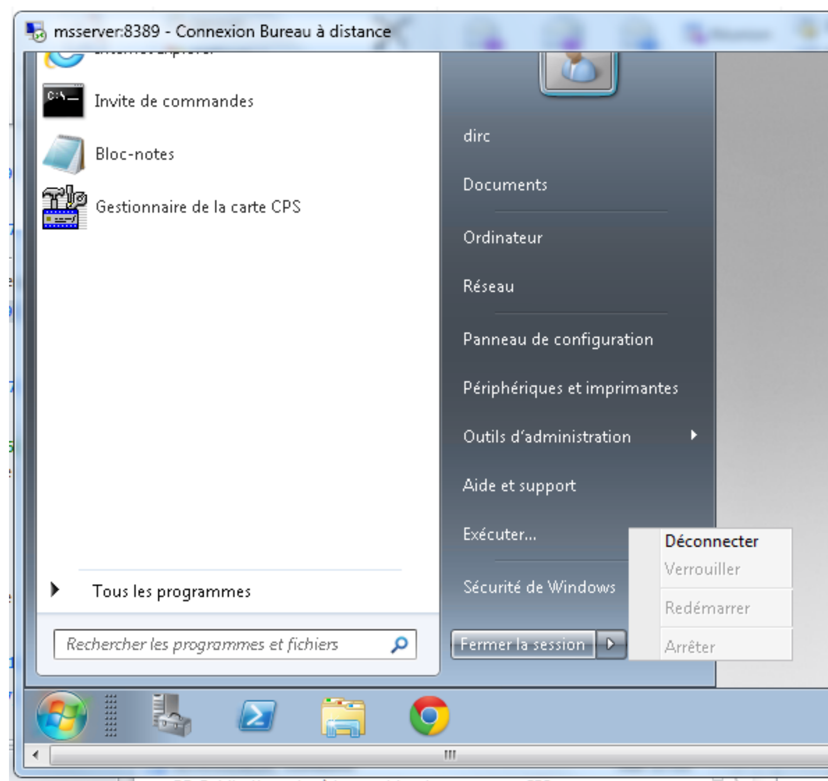


Figure 162 : Workaround : Désactivation verrouillage de session

Il est possible d'affiner le paramétrage de sorte qu'aucune manière de locker la session ne soit accessible ou que plus généralement le cycle de vie de la session utilisateur soit parfaitement maitrisé par l'administrateur système (ce qui est d'ailleurs important dans le cas du Smartcard logon):
Cf. http://msdn.microsoft.com/en-us/library/ms815238.aspx

Cf. http://technet.microsoft.com/fr-fr/library/ee617162%28v=ws.10%29.aspx

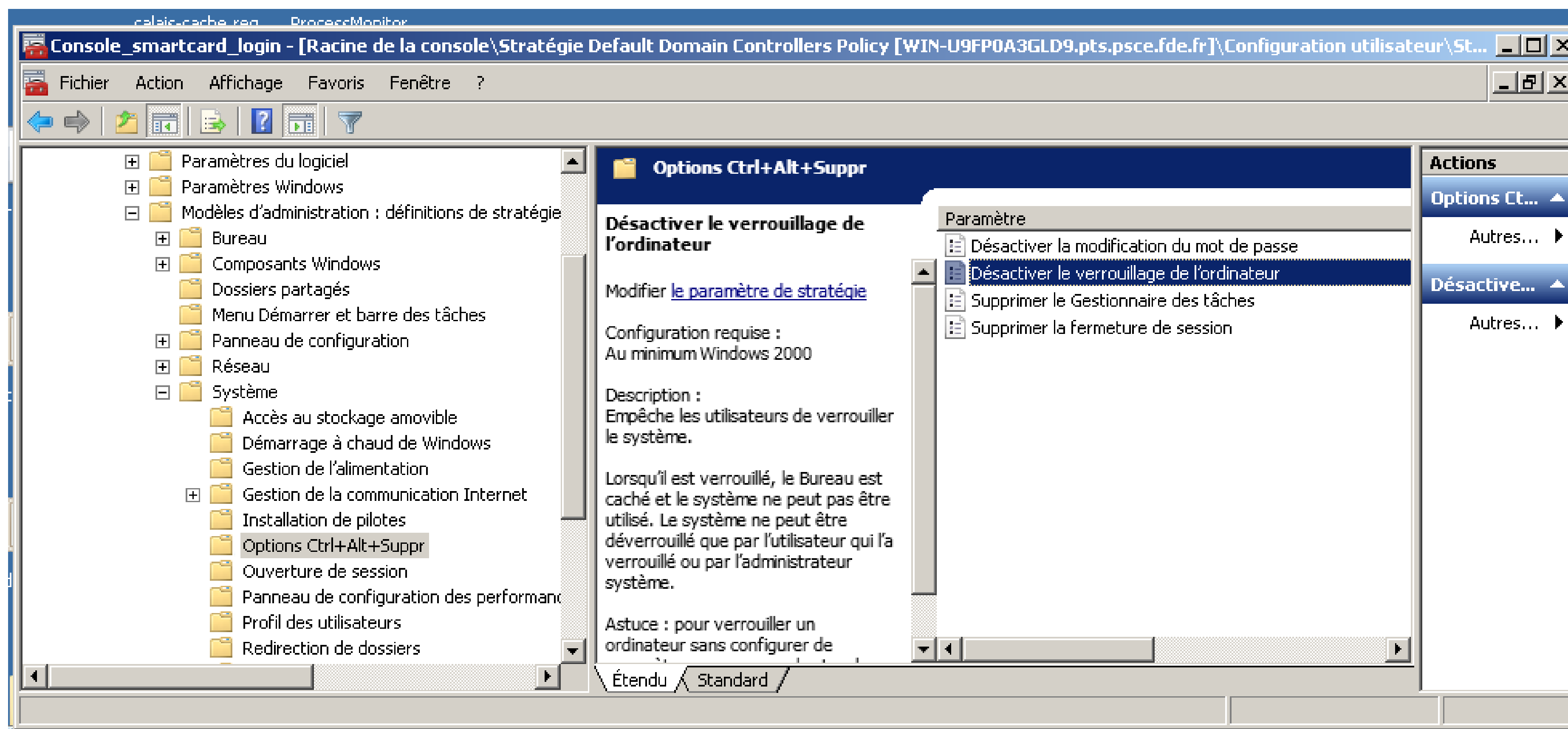


Figure 163 : Workaround : Désactivation verrouillage de session sur Ctrl+Alt+Suppr

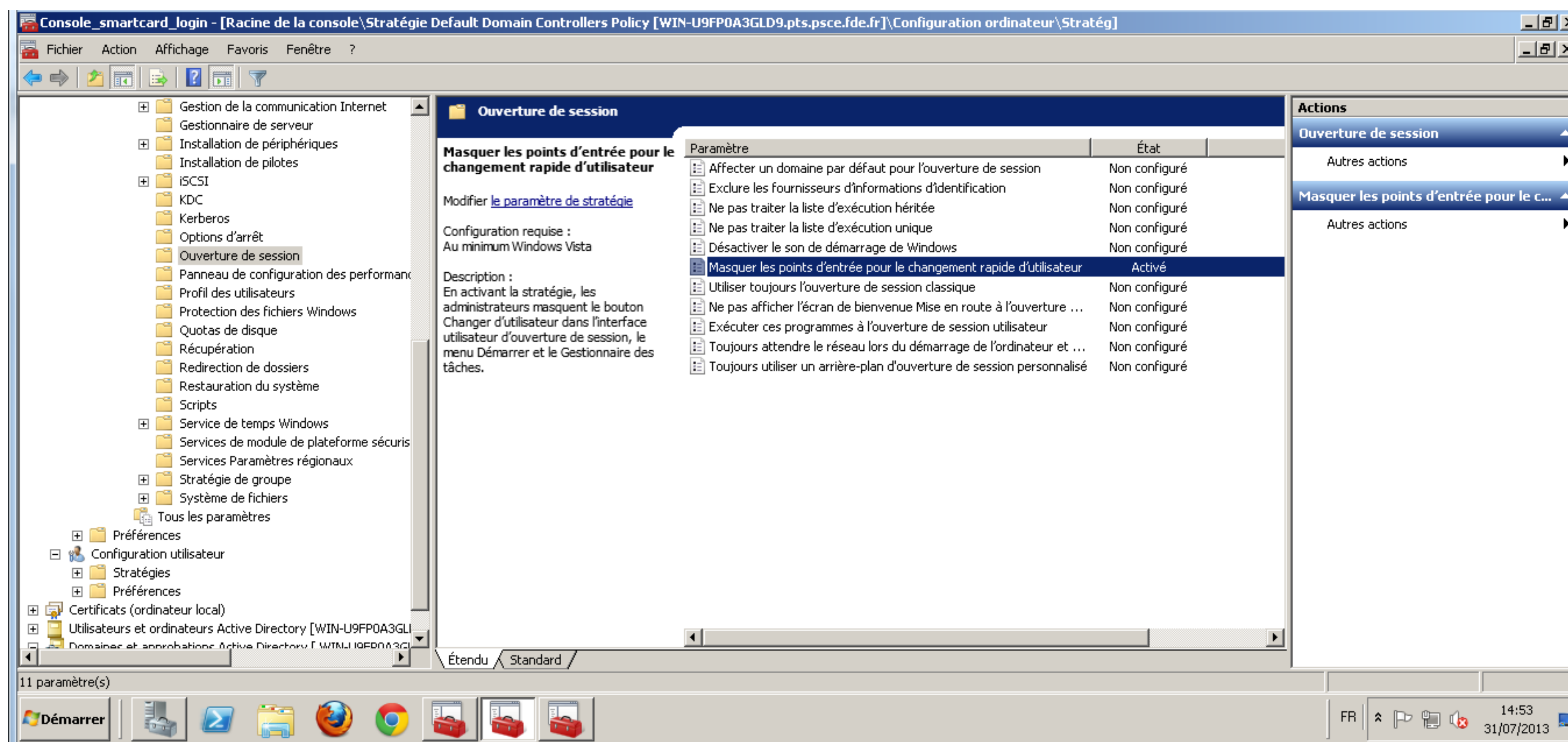


Figure 164 : Workaround : Désactivation changement d'utilisateur

Ne pas oublier la commande « gpupdate » pour propager les nouvelles policies.

13Contenu du « Kit Smartcard logon ASIP Santé »

ID	Répertoire	Description Répertoire	Fichier	Description Fichier
Pack_SCL_0001	bin	Fichiers binaires ou exécutables	00-asipsante-smartcard-logon-ntauth-manage.cmd	Script de peuplement du magasin NTAuth
Pack_SCL_0002	bin		01-asipsante-smartcard-logon-console.msc	Console MMC centralisant les principaux snap-in nécessaires à la configuration des serveurs MS requis pour le Smartcard logon
Pack_SCL_0003	bin		tracelog.exe	Outils de prise de traces MS
Pack_SCL_0004	bin\msi-5.x.y	Installation Cryptolib CPS	Cryptolib-CPS.txt	Lien vers les installeurs MSI de la Cryptolib CPS v5 32b et 64b
Pack_SCL_0005	cer\cer	40 certificats ASIP Santé au format .cer	xx-yy.cer	40 certificats ASIP Santé au format .cer pour peuplement des magasins de certificats
Pack_SCL_0006	cer\p7b	certificats ASIP Santé au format P7B	01-prod-root.p7b	Certificats root de production
Pack_SCL_0007	cer\p7b		02-prod-inter.p7b	Certificats inter. de production
Pack_SCL_0008	cer\p7b		03-test-root.p7b	Certificats root de test
Pack_SCL_0009	cer\p7b		04-test-inter.p7b	Certificats inter. de test

ID	Répertoire	Description Répertoire	Fichier	Description Fichier
Pack_SCL_0010	cer\p7b		05-all-root.p7b	Certificats root de test et de production
Pack_SCL_0011	cer\p7b		06-all-inter.p7b	Certificats inter. de test et de production
Pack_SCL_0012	cer\pem	40 certificats ASIP Santé au format .pem	xx-yy.pem	Fournis par commodité. Peuvent servir aux configurations de profiles Firefox par exemple.
Pack_SCL_0013	cfg	Fichiers de configuration	cps_pkcs11_pcsc.ini	Exemple de fichier de config Cryptolib
Pack_SCL_0014	doc	Documentation et ReleaseNotes	ASIP-PTS-PSCE_Guide-de-mise-en-oeuvre-d-un-smartcard-logon-avec-une-carte-CPS_yyyyMMdd_vX.Y.Z.pdf	Le présent document
Pack_SCL_0015	doc		Guide_de_deploiement_de_louverture_de_session_par_carte_CPSv3_v1.0.pdf	Guide écrit et diffusé par MS
Pack_SCL_0016	leg	Mentions légales	COPYRIGHT.txt	
Pack_SCL_0017	leg		DISCLAIMER.txt	
Pack_SCL_0018	leg		LICENSE.txt	
Pack_SCL_0019	leg		README.txt	
Pack_SCL_0020	log\cryptolib	Pack de prise de traces	debug-cryptolib-activate.reg	Activation des traces de la Cryptolib CPS

ID	Répertoire	Description Répertoire	Fichier	Description Fichier
			debug-cryptolib-deactivate.reg	Désactivation des traces de la Cryptolib CPS
Pack_SCL_0021	log\kerberos-reg		debug-smartcard-logon-kerberos-activate.reg	Activation des traces Kerberos
Pack_SCL_0022	log\kerberos-reg		debug-smartcard-logon-kerberos-deactivate.reg	Désactivation des traces Kerberos via la BdR
Pack_SCL_0023	log\kerberos-tracelog		02-asipsante-smartcard-logon-kerberos-tracelog.cmd	Activation / désactivation des traces Kerberos via tracelog
Pack_SCL_0024	[RACINE]		README.txt	

Tableau 45 : Contenu du « Kit Smartcard logon CPS ASIP Santé»

14 Smartcard logon sous Linux

Il est possible de configurer le PAM Linux pour faire du Smartcard logon.

Ce chapitre décrit les principales étapes à réaliser afin d'effectuer un Smartcard logon local (testé OK sous LUbuntu 12.04 x32 avec la Cryptolib CPS v5 x32 – pas de Cryptolib CPS v5 x64 pour Linux!).

14.1 Installation de la Cryptolib CPS v5 pour Linux

Cf. Manuel d'installation et d'utilisation de la Cryptolib CPS v5.

14.2 Configuration du lancement automatique du daemon PCSCD

# Se référer à :	
Source0	**http://ludovicrousseau.blogspot.fr/2010/12/configuring-your-system-for-pcscd-auto.html**
# En particulier:	
sudo addgroup --system pcscd	
sudo mkdir /var/run/pcscd	
sudo chgrp pcscd /var/run/pcscd	
sudo chmod g+w /var/run/pcscd	

14.3 Installation et configuration du PAM OpenSC

Source1	https://www.opensc-project.org/opensc/wiki/ApplicationSupport
Source2	http://blog.fkraiem.org/2013/03/13/linux-smart-card-authentication-pam/

14.3.1 Récupération et installation de libpam-pkcs11

sudo apt-get install libpam-pkcs11
Début de la configuration
sudo mkdir /etc/pam_pkcs11
sudo mkdir /etc/pam_pkcs11/cacerts
sudo mkdir /etc/pam_pkcs11/crls

14.3.2 Initialisation du fichier pam_pkcs11.conf, des certificats et des CRLs

zcat /usr/share/doc/libpam-pkcs11/examples/pam_pkcs11.conf.example.gz | sudo tee /etc/pam_pkcs11/pam_pkcs11.conf
sudo vi /etc/pam_pkcs11/pam_pkcs11.conf
edit the use_mappers line to list only pwent
copy the certificate of the CA who signed your own certificate (if your certificate is self-signed, that's the certificate itself) into /etc/pam_pkcs11/cacerts and rehash the list of CA certificates with:
sudo cp /etc/opt/santesocial/CPS/Coffre/*.cer /etc/pam_pkcs11/cacerts/
cd /etc/pam_pkcs11/cacerts
sudo pkcs11_make_hash_link

14.3.3 Edition de /etc/pam.d/sudo

sudo vi /etc/pam.d/sudo
contenu normal:
#%PAM-1.0
auth required pam_env.so readenv=1 user_readenv=0
auth required pam_env.so readenv=1 envfile=/etc/default/locale user_readenv=0
@include common-auth
@include common-account
@include common-session-noninteractive
Edition du contenu:
auth required pam_env.so readenv=1 user_readenv=0
auth required pam_env.so readenv=1 envfile=/etc/default/locale user_readenv=0
auth sufficient pam_pkcs11.so
@include common-auth
@include common-account
@include common-session-noninteractive
test with
sudo -i
revert to initial /etc/pam.d/sudo content

14.3.4 Edition de /etc/pam.d/common-auth

sudo vi /etc/pam.d/common-auth
Verifier la ligne:
auth [success=3 default=ignore] pam_pkcs11.so

14.3.5 Edition de /etc/pam_pkcs11/pam_pkcs11.conf

Source3: http://opensc.github.io/pam_pkcs11/doc/pam_pkcs11.html#idp5105696
sudo vi /etc/pam_pkcs11/pam_pkcs11.conf
use_pkcs11_module = cps;
[...]
pkcs11_module cps {
module = /opt/santesocial/CPS/lib/libcps3_pkcs11_lux.so
description = "CPS3";
slot_description = "none";
support_threads = false;
ca_dir = /etc/pam_pkcs11/cacerts;
crl_dir = /etc/pam_pkcs11/crls;
cert_policy = none;
crl_policy = none;
}
[...]
#use_mappers = digest, cn, pwent, uid, mail, subject, null;
use_mappers = subject

14.3.6 Configuration d'un compte pour le Smartcard logon

14.3.6.1 Création d'un utilisateur de test

Définition d'un compte « scl », par exemple :
sudo adduser **scl**
password: **scl**
sudo adduser **scl** root

14.3.6.2 Définition du mapping DN / Compte : /etc/pam_pkcs11/subject_mapping

Lancer la commande :
pklogin_finder
si la carte est bien lue, une ligne du type suivant apparait:
/C=FR/O=GIP-CPS/L=Paris (75)/OU=318751275100020/CN=518751275100020/0000000311/SN=NOM/GN=PRENOM

éditer /etc/pam_pkcs11/subject_mapping:
sudo vi /etc/pam_pkcs11/subject_mapping
ajouter une ligne du type :
/C=FR/O=GIP-CPS/L=Paris (75)/OU=318751275100020/CN=518751275100020/0000000311/SN=NOM/GN=PRENOM -> scl
(chaine DN -> nom du compte)
tester le mapping avec:
pklogin_finder

15Smartcard logon sous Mac OS X

Source0	http://support.apple.com/kb/ta24244
Source1	http://www.charismathics.com/fileadmin/files/pdf/manuals/Mac_Logon.pdf

La fonctionnalité de Smartcard logon est a priori offerte par Mac OS X.

Elle était bien supportée et documentée sur Mac OS X 10.4 Tiger.

Ce n’est plus forcément le cas sur les Mac OS X récents.

La procédure décrite ci-après a été testée sous Mac OS X 10.9 Mavericks.

15.1 Pré-requis

#	Pré-requis au Smartcard logon sous Mac OS X
1	Certificats AC racine dans trousseau « AC Racines »
2	Certificats AC intermédiaires dans trousseau « Système » (ce que l’installeur de la Cryptolib CPS ne fait pas)
3	Lecteur et carte fonctionnent

Tableau 46 : Pré-requis au Smartcard logon sous Mac OS X

15.2 Méthode

```
# Récupérer les hash de clé
$ sc_auth hash
# retour : <cert_auth_hash> : AABB8F7E3E94D924E46550A1A5EEB8DD6F14XXYY par exemple
# Ajouter un hash pour l'authentification (voir « man » pour la suppression d’un hash)
$ sudo sc_auth accept -u <nom_du_compte> -h <cert_auth_hash>
# Autoriser l’authentification par carte à puce (disable pour désactiver)
$ sudo security authorizationdb smartcard enable
```

Tableau 47 : Methode pour appliquer le Smartcard logon sous Mac OS X

15.3 Autres commandes utiles

```
$ sudo sc_auth remove -u <nom_du_compte>
$ sudo sc_auth list -u <nom_du_compte>
```

Tableau 48 : Commandes utiles au Smartcard logon sous Mac OS X

15.4 Remarques

- La configuration avec des comptes réseau est différente
  - Cf. internet pour ces configurations plus spécifiques
- L'authentification par mot de passe n'est pas désactivée
  - Apparemment, il n'est pas possible de le faire
- Ne pas faire les tests trop vite
  - 2 ou 3 secondes peuvent être nécessaires pour que la fenêtre change en « code porteur » à l'insertion de la carte
- Ce cas d'usage semble être peu sponsorisé par Apple

16Annexe – Liste des figures

Figure 1 : Ecran d'accueil de Windows XP, configuré pour ouvrir une session avec une carte à puce. 13
Figure 2 : Ecran d'accueil de Windows 7, configuré pour ouvrir une session avec une carte à puce... 13
Figure 3 : Ecran du client Terminal Server sous Windows 7 pour ouvrir une session avec une carte à puce. 13
Figure 4 : Schéma fonctionnel global du Smartcard logon de Microsoft (Win 2000 et XP) 16
Figure 5 : Schéma fonctionnel global du Smartcard logon de Microsoft (Win Vista+) [7] 17
Figure 6 : Smartcard logon et TSE : Redirection des APDU [1] 22
Figure 7 : Architecture: Exemple d'un réseau informatique configuré pour le Smartcard logon 24
Figure 8 : Exemple d'un certificat de type « Smartcard logon » 28
Figure 9 : Informations des certificats de type « Smartcard logon » 29
Figure 10 : Poste client: Vérifier le certificat d'authentification 31
Figure 11 : Poste client: identifier l'UPN du certificat d'authentification 31
Figure 12 : Poste client: identifier l'UPN du certificat d'authentification 32
Figure 13 : Active Directory: Smartcard logon : Configuration d'un compte utilisateur 34
Figure 14 : Active Directory: Approbation du suffixe UPN « carte-cps.fr » 35
Figure 15 : Forcer l'utilisation de la carte à puce par stratégie locale 37
Figure 16 : Architecture : Exemple d'architecture réseau évoluée 43
Figure 17 : Macro-planning « maquette de Smartcard logon avec une carte CPx » 47
Figure 18 : Poste client : Erreur de carte à puce sur un login TSE si les Cryptolib CPS ne sont pas installées 49
Figure 19 : Poste client : Installation Cryptolib CPS x64 50
Figure 20 : Poste client: Installation Cryptolib CPS x64 : installation perso avec la filière CPS2Ter Full PC/SC 50
Figure 21 : Poste client: Installation Cryptolib CPS x64 : installation perso avec la filière CPS2Ter Full PC/SC 51
Figure 22 : Poste client : Installation Cryptolib CPS x64 : Installer 51
Figure 23 : Poste client: Installation Cryptolib CPS x64 : Fenêtre d'UAC 52
Figure 24 : Poste client : Installation Cryptolib CPS x64 avec AVAST 52
Figure 25 : Poste client : Driver carte à puce OK sur un login TSE (les Cryptolib CPS sont installées) .. 53
Figure 26 : Poste client : Vérifier le magasin de certificats 53
Figure 27 : Poste client : Vérifier le certificat d'authentification 54
Figure 28 : Poste client : identifier l'UPN du certificat d'authentification 55
Figure 29 : Poste client : identifier l'UPN du certificat d'authentification 56
Figure 30 : Poste client : Périphériques et imprimantes : Paramètres d'installation de périphériques et Windows Update 57
Figure 31 : Windows serveur: Installation: choix du type d'installation 58
Figure 32 : Windows serveur: Installation: copie de fichier 59
Figure 33 : Windows serveur: Installation: mot de passe administrateur 60
Figure 34 : Windows serveur: Installation: saisie mot de passe administrateur 61
Figure 35 : Windows serveur: Installation: mot de passe administrateur changé 62
Figure 36 : Windows serveur: Installation: accueil 63
Figure 37 : Windows serveur: Installation: sécurité renforcée 64
Figure 38 : Windows serveur: Installation: Paramétrage de la sécurité renforcée 65
Figure 39 : Windows serveur: Configuration: maitriser les mises à jour 66
Figure 40 : Windows serveur: Configuration: maitriser les mises à jour 67
Figure 41 : Windows serveur: Configuration: nom de l'ordinateur 68
Figure 42 : Active Directory: Installation du rôle 69
Figure 43 : Active Directory: Installation du rôle : résultat 70
Figure 44 : Active Directory: Configuration du rôle 71

Figure 45 : Active Directory: Configuration du rôle : Exécution de l'assistant 72
Figure 46 : Active Directory: Configuration du rôle : mode avancé 73
Figure 47 : Active Directory: Configuration du rôle : nouvelle forêt 74
Figure 48 : Active Directory: Configuration du rôle : nom de domaine 75
Figure 49 : Active Directory: Configuration du rôle : vérification de la disponibilité du nom de la forêt 76
Figure 50 : Active Directory: Configuration du rôle : NetBIOS 77
Figure 51 : Active Directory: Configuration du rôle : Vérif. NetBIOS 78
Figure 52 : Active Directory: Configuration du rôle : Niveau fonctionnel 79
Figure 53 : Active Directory: Configuration du rôle : Configuration DNS 80
Figure 54 : Active Directory: Configuration du rôle : Décocher DNS 81
Figure 55 : Active Directory: Configuration du rôle : mot de passe LDAP 82
Figure 56 : Active Directory: Configuration du rôle : configuration des bases de données 83
Figure 57 : Active Directory: Configuration du rôle : Installation GPMC 84
Figure 58 : AD CS : Installation du rôle 85
Figure 59 : AD CS : service du rôle « Autorité de certification » 86
Figure 60 : AD CS : Type d'installation : Choisir « Entreprise » 87
Figure 61 : AD CS : type d'autorité : Choisir « Autorité de certification racine » 88
Figure 62 : AD CS : Choisir « Créer une nouvelle clé privée » 89
Figure 63 : AD CS : clé privée : Chiffrement 90
Figure 64 : AD CS : clé privée : Préciser le nom de l'AC 91
Figure 65 : AD CS : clé privée : Préciser la période de validité 92
Figure 66 : AD CS : clé privée : Base de données de certificats 93
Figure 67 : AD CS : clé privée : confirmation 94
Figure 68 : AD CS : clé privée : résultats 95
Figure 69 : AD CS: Certificat AD CS 96
Figure 70 : AD CS: Certificat AD CS 97
Figure 71 : AD: Certificat AD deliver par AD CS 98
Figure 72 : AD: Certificat AD DomainController délivré par AD CS 98
Figure 73 : Terminal Server : installation du rôle 99
Figure 74 : Terminal Server : service de rôle : choisir « Hôte de session Bureau à distance » 100
Figure 75 : Terminal Server : mode d'authentification RDP : Choisir « Ne nécessite pas l'authentification au niveau réseau » 101
Figure 76 : Terminal Server : mode de licence : Choisir « Configurer ultérieurement » 102
Figure 77 : Terminal Server : utilisateurs : garder « Administrateurs » 103
Figure 78 : Terminal Server : expérience client 104
Figure 79 : Terminal Server : résultat de l'installation 105
Figure 80 : Terminal Server : Lancer le Gestionnaire des licences des services Bureau à distance 106
Figure 81 : Terminal Server : Clic-droit > propriétés 106
Figure 82 : Terminal Server : Mode de connexion > Navigateur Web 107
Figure 83 : Terminal Server : Configurations des comptes « Serveurs de licences des services Terminal Serveur » 108
Figure 84 : Terminal Server : Fin de l'activation du serveur de licences Terminal Serveur 109
Figure 85 : Terminal Server : Installation d'un pack de licences 110
Figure 86 : Terminal Server : Configuration d'hôte de session Bureau à distance 111
Figure 87 : Terminal Server : Configuration d'hôte de session Bureau à distance > mode de licence et serveurs de licences 112
Figure 88 : Terminal Server : Configuration d'hôte de session Bureau à distance > mode de licence et serveurs de licences 112
Figure 89 : Terminal Server : Configuration des paramètres serveur 113
Figure 90 : Terminal Server : config. nom du serveur et port externe 114
Figure 91 : Terminal Server : Déclaration d'une remote app de test 115

Figure 92 : Terminal Server : Compatibilité ascendante RDP 116
Figure 93 : Terminal Server : Ajout d'utilisateur du bureau à distance 117
Figure 94 : Terminal Server : Groupe utilisateur du Bureau à distance 117
Figure 95 : Terminal Server : Droits d'ouverture de session à distance 118
Figure 96 : Terminal Server : Droits d'ouverture de session à distance pour un utilisateur précis 118
Figure 97 : Terminal Server : Droits d'ouverture de session à distance pour le groupe « Utilisateur du Bureau à distance » 119
Figure 98 : Terminal Server : Création d'un modèle de certificat Remote Desktop sur l'AD CS 120
Figure 99 : Terminal Server : Création d'un modèle de certificat Remote Desktop sur l'AD CS 121
Figure 100 : Terminal Server : Création d'un modèle de certificat Remote Desktop sur l'AD CS 122
Figure 101 : Terminal Server : Création d'un modèle de certificat Remote Desktop sur l'AD CS 122
Figure 102 : Terminal Server : Création d'un modèle de certificat Remote Desktop sur l'AD CS 123
Figure 103 : Terminal Server : Droits sur le modèle de certificat Remote Desktop 123
Figure 104 : Terminal Server : Droits sur le modèle de certificat Remote Desktop 124
Figure 105 : Terminal Server : Déploiement du modèle de certificat Remote Desktop sur les postes clients via l'AD 124
Figure 106 : Terminal Server : Demande de certificat Terminal Server 125
Figure 107 : Terminal Server : Demande de certificat Terminal Server : Sélection de « RemoteDesktopComputer » 125
Figure 108 : Terminal Server : Demande de certificat Terminal Server 126
Figure 109 : Terminal Server : Vérification du certificat Terminal Server émis sur l'AD CS 127
Figure 110 : Terminal Server : Vérification du certificat Terminal Server émis sur le Terminal Serveur 127
Figure 111 : Terminal Server : Installation du certificat Terminal Server 128
Figure 112 : Terminal Server : Configuration 129
Figure 113 : Terminal Server : Installation du certificat Terminal Server 129
Figure 114 : Terminal Server : Installation du certificat Terminal Server 130
Figure 115 : Terminal Server : Vérifier l'installation du certificat Terminal Server 131
Figure 116 : IIS: Installation du rôle 134
Figure 117 : IIS: Installation du rôle : sélection des options de sécurité 135
Figure 118 : IIS: Installation du rôle : état d'avancement 136
Figure 119 : IIS: Installation du rôle : Résultat 137
Figure 120 : CCM: lancement du CCM au démarrage des sessions utilisateurs sur un serveur Windows 138
Figure 121 : CPSRev: répertoire d'installation 139
Figure 122 : CPSRev: résultat d'installation 140
Figure 123 : CPSRev: vérification du magasin Root (Local machine) 141
Figure 124 : CPSRev: vérification du magasin Intermediate CA (Local machine) 142
Figure 125 : CPSRev: vérification du magasin Root CA (User) 143
Figure 126 : CPSRev: vérification du magasin Intermediate CA (User) 144
Figure 127 ; CPSRev : vérification des statuts de certificats offline : consultation du magasin de CRL 147
Figure 128 : Console Enfichable: MMC 151
Figure 129 : Console Enfichable: Ajout de composants enfichables 152
Figure 130 : Console Enfichable: Certificats 153
Figure 131 : Console Enfichable: Certificats utilisateur 154
Figure 132 : Console Enfichable: Certificats Local Machine 155
Figure 133 : Console Enfichable: Certificats Local Machine 156
Figure 134 : Console Enfichable: Stratégie de groupe du contrôleur de domaine 157
Figure 135 : Console Enfichable: Liste des composants utilisés pour le Smartcard logon 158
Figure 136 : Console Enfichable: Sauvegarde 159
Figure 137 : Active Directory: Configuration: Certificat Local Machine personnel 160

Figure 138 : Active Directory: Configuration: Copie de certificats Racine 161
Figure 139 : Active Directory: Configuration: Collage de certificats Racine dans le magasin personnel 162
Figure 140 : Active Directory: Configuration: Magasin NTAUTH avant import 163
Figure 141 : Active Directory: Configuration: Magasin NTAUTH après import 164
Figure 142 : Active Directory: Configuration: Stratégie de clé publique avant import 166
Figure 143 : Active Directory: Configuration: Stratégie de clé publique après import 167
Figure 144 : Active Directory: Configuration: Approbation du suffixe UPN « carte-cps.fr » 170
Figure 145 : Active Directory: Configuration: Définition d'un compte avec Smartcard logon activé . 171
Figure 146 : Active Directory: Configuration: Définition d'un compte avec Smartcard logon activé . 171
Figure 147 : Active Directory: Configuration: Smartcard logon en TSE 172
Figure 148 : Active Directory: Configuration: Bureau à distance et CPS Gestion après Smartcard logon 173
Figure 149 : Paramétrage du Smartcard logon sur des comptes AD préexistants : cas {un compte existant ; une carte} 177
Figure 150 : Active Directory: Configuration du Smartcard logon pour utilisateurs existants 178
Figure 151 : Active Directory: Configuration du Smartcard logon pour utilisateurs existants 179
Figure 152 : Active Directory: Configuration du Smartcard logon pour utilisateurs existants 179
Figure 153 : Active Directory: Configuration du Smartcard logon pour utilisateurs existants 180
Figure 154 : Active Directory: Configuration du Smartcard logon pour utilisateurs existants 180
Figure 155 : Active Directory: Configuration du Smartcard logon pour utilisateurs existants : GPO « Allow user hint » 183
Figure 156 : Comptes existants : Ecran de Smartcard logon après lecture d'une carte 184
Figure 157 : Comptes existants : Saisie du code porteur et du « hint » 184
Figure 158 : Comptes existants : Ouverture de session Windows 184
Figure 159 : Configuration de la Stratégie de retrait de la carte à puce (manuel) 185
Figure 160 : Configuration de la Stratégie de retrait de la carte à puce (passage en automatique) .. 186
Figure 161 : Configuration de la Stratégie de retrait de la carte à puce (automatique) 187
Figure 162 : Workaround : Désactivation verrouillage de session 211
Figure 163 : Workaround : Désactivation verrouillage de session sur Ctrl+Alt+Suppr 212
Figure 164 : Workaround : Désactivation changement d'utilisateur 213

17Annexe – Liste des tables

Tableau 1 : Glossaire 9
Tableau 2 : Entreprises citées..... 10
Tableau 3 : Avertissements 11
Tableau 4 : Inconvénients du couple login/mot de passe..... 14
Tableau 5 : Avantages de la carte à puce 14
Tableau 6 : Inconvénients de la carte à puce face au couple login/mot de passe..... 15
Tableau 7 : Smartcard logon: Principaux Composants Microsoft mis en œuvre 18
Tableau 8 : Smartcard logon: Protocole Kerberos 20
Tableau 9 : Smartcard logon: Cinématique de l'authentification par carte à puce 21
Tableau 10 : Smartcard logon: Cinématique de l'authentification par carte à puce 23
Tableau 11 : Architecture: Scénarios d'implémentation de PKI serveur 25
Tableau 12 : CPSRev : désactivation de la vérification des CRLs..... 39
Tableau 13 : Serveur: Installation du serveur 40
Tableau 14 : Serveur: Configuration..... 42
Tableau 15 : « Brief Project » « maquette de Smartcard logon avec une carte CPx »..... 44
Tableau 16 : Ressources « maquette de Smartcard logon avec une carte CPx » 45
Tableau 17 : Livrables « maquette de Smartcard logon avec une carte CPx » 46
Tableau 18 : Macro-planning « maquette de Smartcard logon avec une carte CPx »..... 46
Tableau 19 : Remarques « maquette de Smartcard logon avec une carte CPx » 48
Tableau 20 : CPSRev : Configuration de CPSRev pour prise en compte des certificats de test ASIP Santé..... 145
Tableau 21 : CPSRev : Désactivation de la vérification des listes de révocation sous Win2008+..... 145
Tableau 22 : CPSRev : (Ré-)Activation de la vérification des listes de révocation sous Win2008+..... 145
Tableau 23 : CPSRev : Vérification des flux vers l'annuaire ASIP Santé 146
Tableau 24 : CPSRev : Ligne de commande certmgr.exe 146
Tableau 25 : CPSRev : Résultat de la vérification d'un certificat avec CPSRev..... 150
Tableau 26 : Active Directory: Configuration: Commande certutil d'import des certificats dans le magasin NTAUTH..... 165
Tableau 27 : Déploiement UPN : Construction de l'UPN 169
Tableau 28 : Déploiement UPN : Exemple de script VBS permettant la modification de l'UPN d'utilisateurs existants dans un annuaire Active Directory..... 175
Tableau 29: Déploiement UPN : Exemple de Fichier « users.txt »..... 175
Tableau 30 : Déploiement UPN: Exemple de script VBS permettant la création d'utilisateurs dans un annuaire Active Directory..... 176
Tableau 31 : Liste des possibilités de mapping user / certificat pour l'authentification par certificat181
Tableau 32 : Désactivation de l'utilisation du SubjectAltName (SAN) 182
Tableau 33 : Activation du « hint »..... 182
Tableau 34 : Active Directory: Configuration du Smartcard logon pour utilisateurs existants : Références..... 183
Tableau 35 : Comptes existants : Considération d'ergonomie en Smartcard logon sur compte préexistant..... 184
Tableau 36 : Liste de certificats..... 200
Tableau 37 : Activation des traces Kerberos via la base de registre 201
Tableau 38 : Activation des traces Kerberos via la base de registre 201
Tableau 39 : Emplacement des traces Kerberos après activation via la base de registre 202
Tableau 40 : Désactivation des traces Kerberos activées via la base de registre 202
Tableau 41 : Activation des traces Kerberos via Tracelog..... 203
Tableau 42 : Emplacement des traces Kerberos après activation via Tracelog 203
Tableau 43 : Désactivation des traces Kerberos activées via Tracelog 203

Tableau 44 : Points d'attention 210
Tableau 45 : Contenu du « Kit Smartcard logon CPS ASIP Santé» 216
Tableau 46 : Pré-requis au Smartcard logon sous Mac OS X........ 220
Tableau 47 : Methode pour appliquer le Smartcard logon sous Mac OS X 220
Tableau 48 : Commandes utiles au Smartcard logon sous Mac OS X 220

18Notes

[fin du document]





Agence des systèmes d'information partagés de santé
9, rue Georges Pitard - 75015 Paris
Tel : 01 58 45 32 50
esante.gouv.fr